СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(17.10–30.10)

2016 № 13

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(17.10–30.10)
№ 13

Засновники:
Національна бібліотека України імені В. І. Вернадського
Служба інформаційно-аналітичного забезпечення
органів державної влади (СІАЗ)

Відповідальний редактор
Л. Чуприна, канд. наук із соц. комунікацій

Упорядник
І. Терещенко

Заснований у 2011 році
Виходить двічі на місяць

Київ 2016

ЗМІСТ

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ

17.10.2016
Twitter запускает функцию Periscope Producer

Новая функция для брендов, медиа организаций и других производителей онлайн-видео позволит делиться высококачественным видеоконтентом в Periscope и Twitter. С ее помощью партнеры сети смогут транслировать видео в высоком качестве, используя внешние камеры и соответствующий софт. При этом им также будут доступны все функции вовлечения пользователей, существующие в Periscope и Twitter. «Дать людям инструменты, которые позволят создавать и делиться специально произведенным онлайн-видео в Periscope, всегда было частью концепции нашего развития. Этот шаг откроет для пользователей возможность смотреть разные виды видеоконтента в режиме онлайн, – говорит Кейвон Бейкпур, генеральный директор Periscope. – Теперь платформа позволяет всем смотреть рейтинговые видеотрансляции – популярные ежедневные шоу, крупномасштабные и небольшие события и другой увлекательный контент от производителей, которых они знают и любят. А с помощью всего лишь одного твита можно будет поделиться высококачественным генерируемым видео». Используя профессиональные камеры и стриминговый софт, производители видеоконтента смогут легко создавать и транслировать в Periscope онлайн-видео более высокого качества. Такие партнеры компании как ABC’s Dancing with the Stars, Estadao, Fusion, Louis Vuitton, The News & Documentary Emmy Awards, The Ringer, XBox UK и Walt Disney Studios уже увеличили вовлечение и нарастили свою аудиторию с помощью своего видеоконтента в Periscope и Twitter (Marketing Media Review).

***

17.10.2016
Видео из Facebook теперь можно транслировать через Apple TV и Google Chromecast

Видео из Facebook теперь можно транслировать через мультимедийные проигрыватели Apple TV и Google Chromecast. Таким образом, ролики из социальной сети, наконец, можно смотреть не только на маленьком экране компьютера, но и на большом телевизоре (InternetUA).

Поддержка Apple TV, а также других совместимых с технологией AirPlay устройств доступна уже сейчас. Обладатели Chromecast могут транслировать видео с устройств на базе iOS или через веб-браузер – поддержка воспроизведения с Android появится «скоро».

Для того чтобы просмотреть какой-либо ролик из Facebook на большом экране, достаточно нажать на иконку телевизора, расположенную в правом

верхнему углу, и выбрать устройство, на котором будет воспроизводиться видео. Во время просмотра можно будет комментировать ролик и оставлять «реакции» с телефона или компьютера, причём на телевизоре будут видны и действия других пользователей.

Транслировать на Apple TV или Chromecast можно абсолютно любое видео, включая прямые трансляции Facebook Live. В последнем случае, правда, процесс запускается с мобильного устройства, поэтому с персонального компьютера запустить прямую трансляцию на большом экране не получится.

Более 100 миллионов часов видео просматривается в Facebook каждый день. Для социальной сети это имеет огромное значение – особенно если учесть, что она конкурирует с Twitter, YouTube и Snapchat не только в плане внимания пользователей, но и в плане лучших авторов контента. Теперь, когда видео из социальной сети можно смотреть на телевизорах, в Facebook могут начать появляться и более длинные видео вроде спортивных передач и даже фильмов.

***

19.10.2016

Пользователям Viber будет проще делиться своими впечатлениями

Пользователям устройств под управлением Android и iOS доступен обновленный интерфейс мобильного приложения Viber (ITnews).

Благодаря новому дизайну меню общаться в нем будет еще проще и удобнее. Так, отправить собеседнику фотографию или видеоролик теперь можно вдвое быстрее, чем в предыдущей версии или других мессенджерах, – всего в три касания. Это значит, что поделиться памятными моментами теперь можно буквально за пару секунд.

В новом меню будут доступны следующие функции:

– в версии для iOS: меню стикеров, фотогалерея, фото и видеосъемка, doodle;

– в версии для Android: меню стикеров, фотогалерея, фото и видеосъемка.

Кроме того, дополнительные возможности, такие как отправка файлов и информации о местоположении, будут доступны при нажатии на кнопку «Больше».

***

18.10.2016

Базиленко Анна

Snapchat випередив Instagram і Facebook за популярністю серед підлітків

Згідно з даними звіту Piper Jaffray, 80% американських підлітків щонайменше раз на місяць користуються месенджером Snapchat. Восени 2015 року ця цифра становила 74%, передає Adweek (Watcher).

Instagram відстає від Snapchat лише на 1%: цей сервіс щомісяця використовують 79 % підлітків, що на 3 % більше, аніж у 2015 році (76 %). Що стосується Facebook, лише 52 % респондентів щомісяця відвідують соцмережу. Восени 2015 року ця цифра становила 56 %. Дані звіту засвідчують: наразі Snapchat є найпопулярнішою соціальною платформою серед підлітків.

Серед 14-річних респондентів 80 % щомісяця відвідують Instagram, трохи менше 80 % – Snapchat, 30 % – Facebook і близько 50 % – Twitter. Серед 18-річних – трохи більше 80 % щомісяця відвідують Snapchat, трохи менше 80 % – Instagram, близько 60 % – Facebook, 50 % – Twitter.

Популярність Twitter серед підлітків у всіх вікових групах впала з 58 % у 2015 році до 56 % в 2016. Показники зростання Pinterest залишилися без змін – 25 %. Google+ щомісяця використовують 22 % підлітків.

У відповідь на питання, яка соціальна платформа є улюбленою, 35 % респондентів вказали Snapchat (у 2015 році – 17 %), 24 % – Instagram (у 2015 році – 29 %), 13 % – Facebook і ще 13 % – Twitter.

***

18.10.2016

Facebook начал помогать пользователям удачно завязать разговор

Пользователи мессенджера Facebook обратили внимание на новую функцию: в списке контактов под именами собеседников начали появляться пометки о том, с чего лучше начать разговор с этим человеком. Об этом сообщает TechCrunch (InternetUA).

Чтобы подтолкнуть «френдов» к разговору, мессенджер указывает последние действия пользователя, места, в которых тот недавно побывал, песни, только что им прослушанные, или планируемые мероприятия.

Аватарки людей, с которыми у человека потенциально могут найтись общие интересы, сгруппированы в специальном блоке внутри списка контактов.

TechCrunch предполагает, что функцию тестируется на ограниченном количестве пользователей, пользующихся iOS. Будет ли она доступна для широкой аудитории, пока неизвестно.

По данным Facebook, число активных пользователей мессенджера превышает 900 миллионов в месяц.

***

19.10.2016

Разозлившая Facebook функция появилась во «ВКонтакте»

Администрация «ВКонтакте» внедрила автоматический запуск видеороликов в лентах новостей пользователей, а также на страницах профилей и сообществ. Информация об этом появилась в официальном блоге соцсети (InternetUA).

В настоящее время автозапуск видео доступен в браузерной версии сайта, а в скором будущем нововведение будет реализовано в мобильных приложениях для iPhone и Android.

Качество видео подбирается, исходя из скорости интернет-соединения. Звук во время автозапуска не проигрывается – включить его можно, нажав на сам ролик. При желании пользователи могут отключить автоматическое воспроизведение или же указать в настройках, на каком типе соединения его можно использовать.

***

19.10.2016

Facebook добавил возможность планировать live-видео

Facebook добавил возможность устанавливать таймер для начала трансляции live-видео, отмечает likeni.ru. Функция будет запущена в течение неделе для верифицированных пользователей. Остальные получат доступ к «планированию» live-трансляций чуть позже. Когда вы планируете live-видео, пост с анонсом публикуется в новостной ленте, чтобы сообщить подписчикам, что трансляция скоро начнется. Пользователи, увидевшие пост, могут включить разовое напоминание, которое предупредит их о начале трансляции. Перед началом трансляции ваши подписчики могут собраться в специальной группе для обсуждения видео, – отмечают в блоге Facebook Media.

Воспользоваться функцией планирования трансляций владельцы верифицированных страниц могут с помощью раздела Publishing Tools (Marketing Media Review).

***

20.10.2016

В Киеве презентовали соцсеть для перевозчиков

В Киеве презентовали инновационную онлайн-платформу для перевозчиков A2b Direct. Идея создания сервиса принадлежит бывшему министру транспорта Украины, бизнесмену Евгению Червоненко. Программа позволяет грузоперевозчику и грузообладателю общаться напрямую без посредников и обеспечивает весь документооборот, страховое и юридическое сопровождение груза (podrobnosti.ua).

С октября платформа работает в тестовом режиме а уже в следующем году будет доступна для пользователей ближнего зарубежья.

«Регистрируются в системе только истинные владельцы грузовиков у которых это собственность или аренда – с паспортом, со всем. Кроме этого существует рейтинг, который говорит – ты добросовестный участник рынка? Это ставят грузодержатели другие, точно так же как перевозчик ставит рейтинг грузодержателю 20 октября – это день рождения транспортного Фейсбука», – говорит Евгений Червоненко, бывший министр транспорта Украины.

***

24.10.2016

В Facebook Messenger для Windows 10 появилась возможность совершать звонки

Компания Facebook выпустила обновление своего фирменного мессенджера Messenger для Windows 10, добавив долгожданную возможность совершать аудио- и видеозвонки. Данная функция уже давно доступна на iOS и Android, а теперь появилась и на всех устройствах под управлением Windows 10. Чтобы совершить звонок, необходимо выбрать контакт, который сейчас в сети, а затем нажать на кнопку камеры или телефона в зависимости от того, каким именно способом вы хотите связаться с этим человеком. Звонки осуществляются через Интернет, поэтому для нормального качества нужно стабильное и быстрое соединение (InternetUA).

Представители Facebook сообщают, что они только начали рассылать обновление, поэтому оно может быть ещё не доступно во всех регионах, но в ближайшее время все смогут воспользоваться новыми функциями. Кроме этого, компания также выпустила обновление Messenger для Windows Phone, добавив поддержку видеозвонков. Правда, это пока тестовая сборка, которая доступна небольшому числу пользователей.

***

24.10.2016

В десктопную версию WhatsApp добавили поддержку поиска по чатам

Помимо обновления Messenger для Windows 10, компания Facebook выпустила новую версию WhatsApp для персональных компьютеров. Напомним, десктопное приложение WhatsApp по сути является оболочкой для веб-версии сервиса, которая просто запускается в отдельном окне. В обновлении до версии 0.2.2234 разработчики внесли ряд исправлений и добавили несколько новых функций, в том числе долгожданную возможность поиска по чату. Теперь найти нужное сообщение, адрес или номер телефона в переписке стало гораздо проще (InternetUA).

Изменения в новой версии WhatsApp для Windows 10:

– новые смайлики;

– кнопка для выбора и отправки GIF-анимаций;

– возможность просматривать отправленные изображения;

– поиск внутри чатов;

– улучшения пользовательского интерфейса.

***

21.10.2016

Facebook Messenger и WhatsApp названы самыми защищенными мессенджерами

Правозащитная организация Amnesty International опубликовала собственный рейтинг защищенности мессенджеров от взлома. В список попали 11 компаний, являющихся разработчиками 16 наиболее популярных сервисов (IGate).

Список возглавили WhatsApp и Facebook Messenge, принадлежащие компании Facebook. Приложения были оценены по 100-бальной шкале в 73 балла. Следом за ними идут FaceTime и iMessage от Apple, набравшие 67 баллов. Такое же количество баллов получил и Telegram, но расположился почему-то на третьем месте.

Основным критерием, на который обращали внимание специалисты Amnesty International, было наличие шифрования. Только у шести мессенджеров, из представленных в списке, активна функция end-to-end-шифрования по умолчанию, при использовании которой переписка хранится в зашифрованном виде на конечном устройстве: iMessage, WhatsApp, FaceTime, Duo, Line, а также Viber. В Facebook Messenger и Telegram end-to-end шифрование не применяется по умолчанию.

Отметим, что глава Telegram Павел Дуров осудил исследование Amnesty International, назвав организацию «пиар-инструментом корпораций и правительств».

«Грустно наблюдать за тем, как «неправительственная организация» используется, пиар-инструментом для правительств и крупных корпораций. Говоря, что Facebook, являющийся частью программы PRISM и получающий по 100 тысяч правительственных запросов ежегодно, идеален для приватного общения, Amnesty держит общественность за идиотов», – написал Дуров на своей странице в Twitter.

***

24.10.2016
Базиленко Анна
Facebook обіцяє пом’якшити цензуру і репресії проти користувачів

Facebook готовий скорегувати стандарти спільноти, зокрема, обмежити цензурування матеріалів, які зазвичай видалялися за порушення цих стандартів. У компанії обіцяють, що зміни стануть відчутними вже за кілька тижнів (Watcher).

Політика Facebook і надалі відображатиме інтереси спільноти, запевняють у компанії.

«Наша мета – дозволити більше зображень та історії, при цьому не створюючи загрози неповнолітнім та іншим особам, які не хочуть бачити подібні матеріали», – йдеться в офіційному блозі соцмережі.

Які саме зміни будуть внесені в стандарти спільноти у Facebook не пояснюють, але розраховують на співпрацю з видавцями, журналістами, фотографами, правоохоронцями та адвокатами.

***

24.10.2016

Facebook оповестит пользователей в случае слежки за ними спецслужбами

Facebook оповестит пользователей в случае слежки за ними спецслужбами. Разработчики социальной сети уверены, что с помощью нововведения юзеры смогут получать доказательства того, что за ними ведется наблюдение. Об этом проинформировали представители компании Facebook (HiTech-News.ru).

Пользователям социальной сети Facebook будут рассылаться специальные уведомления в том случае, если их начнет отслеживать кто-либо. По словам разработчиков, благодаря нововведению юзеры получат уверенность в том, что, в случае, если за ними велось наблюдение, в том числе, спецслужбами, они смогут получить доказательства этого, и воспользоваться ими, если дело дойдет до суда.

Новая функция уже доступна в социальной сети Facebook, однако пользоваться ею могут пока не все, а лишь отдельные юзеры. Тем не менее, разработчики пообещали, в скором времени услугу предоставят всем желающим.

В данное время система уведомлений о слежке спецслужб в Facebook находится в состоянии совершенствования. Каким образом работает алгоритм функции, в компании не говорят.

***

21.10.2016

В ICQ добавили возможность обработки видео при помощи нейросетей

Некогда популярный мессенджер ICQ обзавелся функцией обработки видео нейросетями. Кроме того, приложение получило поддержку голосовых лайвчатов (IGate).

В августе 2016 года ICQ стал первым мессенджером, получившим возможность обработки фотографий при помощи нейросетей. Теперь же интеллектуальные алгоритмы научились обрабатывать и видеосообщения, которые можно будет загружать в соцсети и делиться ими в «Историях». Данная функция работает на базе технологий популярного приложения Artisto.

Также разработчики внедрили в мессенджер голосовые «живые» чаты, в которых пользователи смогут обмениваться с собеседниками короткими аудиосообщениями.

Обновленная версия приложения уже доступна для Android-устройств.

***

27.10.2016
«ВКонтакте» может начать брать деньги за музыку

Компания Mail.ru Group рассматривает возможность введения платной музыкальной подписки в своих продуктах. Об этом заявил новый генеральный директор компании Борис Добродеев в ходе телефонной конференции (InternetUA).

Он подчеркнул, что «опции бесплатного прослушивания музыки должны оставаться для пользователей», но в то же время Mail.ru Group намерена начать экспериментировать с монетизацией, включая подписную модель, сообщает «Интерфакс».

В Mail.ru Group информагентству сообщили, что эксперименты с монетизацией коснутся только дополнительных услуг, в то время как базовая функциональность, к которой привыкли пользователи (например, прослушивание музыки «ВКонтакте»), останется бесплатной.

***

26.10.2016
В WhatsApp для Android начали внедрять видеозвонки

Команда сервиса WhatsApp начала внедрять функцию видеозвонков в приложение для Android. Об этом сообщил ресурс Android Police, отметив, что новая функциональность начала появляться у пользователей последних бета-версий WhatsApp для Android в случайном порядке (InternetUA).

При попытке сделать звонок через WhatsApp пользователи видят две опции – голосовой звонок и видеозвонок. У вызываемого пользователя должна быть установлена такая же версия приложения, чтобы можно было начать звонок.

Как сумели выяснить авторы Android Police, появление функции видеозвонка в своем Android-приложении WhatsApp можно ускорить, если стереть данные и залогиниться заново. Такой трюк можно попробовать, но не забудьте сначала сделать бэкап чатов.

***

26.10.2016
Индия стала самым быстрорастущим рынком Facebook

По словам вице-президента Facebook по управлению продуктами Адама Моссери (Adam Mosseri), социальная сеть развивается в Индии быстрее, чем в остальных странах мира. Годовой рост сервиса в Индии составил 22 %, в то время как глобальный рост социальной сети достиг отметки в 17 %. В Индии

Facebook имеет более 155 млн ежемесячных активных пользователей, 77 млн из которых заходят в социальную сеть каждый день. Ежемесячно 147 млн из них заходят в Facebook с телефонов, 73 млн – ежедневно (InternetUA).

Топ-менеджер компании напомнил, как много возможностей Facebook видит в Индии, и рассказал, как компания собирается развиваться в стране. «Наша первичная цель сейчас – принести в онлайн очередной миллиард людей, и Индия, очевидно, является большой его частью», – рассказал Моссери ежедневному индийскому бизнес-изданию Live Mint.

Несмотря на то, что в плане пользователей Сети Индия является одним из самых быстрорастущих рынков, многие жители страны ещё не добрались до Интернета. «Мы не уверены, имеют ли доступ к онлайну хотя бы две трети населения Индии», – заявил представитель Facebook.

Популярность Интернета быстро растёт в более или менее крупных городах страны, однако в более мелких населённых пунктах ситуация значительно хуже. «Мы так сильно беспокоимся об Индии, потому что это важный рынок, который растёт с таким большим темпом. Он также сильно отличается от всех рынков, на которых я фокусировался ранее. Сети, язык, фрагментация контента – всё это совсем другое. В некотором смысле мы больше фокусируемся на сельских районах», – сказал Моссери.

За последние несколько лет многие продукты Facebook стали куда менее громоздкими, благодаря чему к ним стало проще получить доступ с помощью медленного Интернета. Компания также выпустила ряд облегчённых приложений вроде Facebook Lite и Facebook Messenger Lite.

Компания собирается добавить в свои продукты поддержку большего числа языков. Facebook сейчас доступна на 12 региональных языках, при этом около 90 % индийцев не владеют английским языком. Однако, вероятно, главная цель компании – это предоставление жителям страны более качественного интернет-соединения. В прошлом году Facebook запустила в Индии инициативу Free Basics, предоставляющую людям бесплатный доступ к некоторым сайтам и сервисам. Тем не менее, индийское правительство закрыло инициативу из-за её «ограниченного подхода». Поэтому компания начала тестировать новую программу под названием Express Wi-Fi в некоторых отдалённых районах Индии. В частности, Facebook объединится с государственным учреждением RailTel для предоставления доступа к Сети на железнодорожных станциях и в близлежащих регионах.

***

26.10.2016

«ВКонтакте» позволила устанавливать приложения в сообществах

Социальная сеть «ВКонтакте» открыла доступ к платформе приложений сообществ (InternetUA).

Администраторы пабликов и групп могут подключить приложения для покупки товаров, регистрации на мероприятие, записи к врачу и другим услугам.

Сервисы можно выбрать в каталоге в настройках управления сообществом. Также паблики могут разрабатывать собственные приложения с необходимым функционалом.

«Платформа полностью открыта для всех, мы призываем разработчиков придумывать новые форматы и реализовывать самые смелые идеи», – отметил руководитель продукта «Приложения» «ВКонтакте» Максим Павлов.

***

26.10.2016

Facebook розробляє додаток, який перетворює відео на відомі картини

Компанія Facebook наразі працює над додатком для камери, який, використовуючи штучний інтелект, стилізує відео під знамениті малюнки в реальному часі (Espreso.tv).

Можливості цієї програми продемонстрував директор з розробки продуктів компанії Кріс Кокс під час онлайн коференції Wall Street Journal, повідомляє Mashable.

Зазначений додаток дозволить відтворити стиль мистецьких витворів таких художників, як Моне або Рембрандт, накладаючи подібні до цих картин елементи на відео, яке користувач знімає у реальному часі.

«Це дуже цікаво, адже програма використовує вже відому технологію, але використовує її на вашому гаджеті набагато швидше, а також здатна працювати при досить низькій латентності (швидкості виконання команд пристроєм, яка, зазвичай, знижується при роботі з масивними додатками), тому у вас не будуть виникати проблеми з якістю зйомки», – наголосив Кокс.

Наразі невідомо, коли Facebook випустить цей додаток, втім Кокс зазначив, що над цією технологією ведуться роботи.

***

29.10.2016

Алгоритм новостной ленты Facebook не может справиться с фейковыми новостями

Алгоритм новостной ленты Facebook, предназначенный для борьбы с недостоверной информацией, не справляется с поставленной программистами компании целью, передает BuzzFeed (InternetUA).

Сообщается, что планы Facebook по расширению своей роли в предоставлении новостного контента для своих пользователей могут столкнуться с рядом технических проблем.

«Автоматическая проверка фактов и обнаружение недостоверной информации в новостной ленте является очень сложной задачей при создании алгоритма», – заявил специалист в области информатики из Индианского университета. Он добавил, что программисты все еще очень далеки от решения данной задачи.

***

30.10.2016
Microsoft создает на основе Windows 10 социальную сеть MyPeople

Корпорация Microsoft представила масштабное обновление Windows 10. В частности, в обновленной версии операционной системы появится функция MyPeople, которая позволит размещать избранные контакты непосредственно на рабочем столе (InternetUA).

Таким образом в Microsoft планируют облегчить обмен сообщениями как по почте, так и через приложения. Пользователи обновленной Windows 10 также смогут обмениваться эмодзи.

С помощью функции MyPeople пользователь может обозначать важные контакты. Иконки с изображением этих контактов будут находиться на панели задач. Пользователь сможет отправить любой файл, перетащив его на иконку. Таким образом, файлами можно будет делиться с другими пользователями через имейл или Skype.

Обновленная Windows 10 также будет сортировать входящие сообщения с имейлов и чатов в Skype: сообщения от избранных контактов будут появляться в первую очередь. MyPeople позволяет переключаться между приложениями и отвечать в нескольких из них одновременно.

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

17.10.2016
Базиленко Анна
Українці долучились до міжнародного флешмобу на підтримку невиліковно хворих дітей

З нагоди Всесвітнього дня дитячої паліативної допомоги українці долучилися до міжнародного флешмобу #КапелюхаНаВуха (#HatsOn4CPC), мета якого підтримати невиліковно хворих дітей (Watcher).

За даними Міністерства охорони здоров'я, в Україні паліативної допомоги потребують 17 тисяч дітей. Водночас за розрахунками ЮНІСЕФ, їхня

кількість значно більша і становить від 39 до 70 тисяч. Разом з тим, через відсутність реєстрації в Україні немає дитячих форм знеболювального.

Долучитись до флешмобу може кожен охочий, одягнувши шапку (або картуз, капелюха, панамку тощо) та опублікувавши своє фото на сторінці у соціальних мережах із хештегами #КапелюхаНаВуха або #HatsOn4CPC.

***

26.10.2016

«Не вкладається в голові, …». Реакція соцмереж на візит Савченко до Москви

У соціальних мережах активно обговорюють візит Надії Савченко до Росії (Espreso.tv).

Еспресо зібрало реакцію журналістів, громадських діячів з цього приводу.

Нагадаємо, що Надію Савченко, яка вирушила до Москви на апеляцію на вирок українським політв'язням Миколі Карпюку і Станіславу Клиху, двічі затримували російські прикордонники.

Український експерт-політолог, історик Олександр Палій в ефірі Еспресо розповів, що поїздка Савченко до Москви пов'язана з тим, що у неї останнім часом йде провал за провалом. Палій згадав, як нещодавно вона, виступаючи а одному з ефірів сказала, що необхідно повернути Януковича, та пов'язав це з тим, що Савченко свого часу підтримувала антимайдан.

***

28.10.2016Інше

У соцмережі Facebook набирає обертів флешмоб на підтримку Дмитра Міхальця. Патрульний подякував франківцям за підтримку

У соцмережі Facebook франківчани розміщують дописи із хештегом #підтримуюМіхальця, повідомляє Франик.

В такий спосіб вони показують свою підтримку керівнику франківської поліції, якому оголосили підозру у скоєнні правопорушення, за яке йому загрожує від трьох до восьми років ув’язнення.

«Дмитро Міхалець для мене особисто є людиною, яка символізує зміни. Ці зміни він найкраще продемонстрував, коли не погодився “порішати”. Звичайно, ідеальних людей не існує. В такій непростій ситуації я поважаю і #підтримуюМіхальця», – написала Іванна Габльовська.

«Не вірю судам, не вірю прокуратурам, але патрульній поліції вірю. Допоки я не засумнівалась, допоки вони не підірвали мою довіру – буду вірити. Бачу роботу, бачу результат.

І я #підтримуюМіхальця, бо цю людину знаю з першого дня в Івано-Франківську. Підтримую і бажаю вам сили та терпіння. Вважаю, що просто взяти і здатись ми не можемо. Коли хтось використовує когось – ганьба таким людям.

Триває велика гра. Хочу, щоб вона завершилась. Щоб кожний шкідник заспокоївся і дав спокій тим, хто працює», – наголосила Лідія Бойко.

28 жовтня керівнику франківської патрульної поліції Дмитру Міхальцю обрали запобіжний захід – у вигляді особистого зобов'язання та залишили на посаді на час слідчих дій. Міхалець повинен до 25 грудня з'являтися до слідчого на вимогу, інакше йому загрожує штраф.

«Я вас не зраджу», – подякував суду за об'єктивне рішення і за підтримку суспільства Міхалець.

Також головний патрульник запевнив, що ховатися від суду він не буде, навпаки, сумлінно виконуватиме свої обов'язки та забезпечуватиме правопорядок у місті.

***

27.10.2016

Як соцмережі відреагували на мінімалку 3200 грн

Кабінет міністрів планує встановити розмір мінімальної зарплати на рівні прожиткового мінімуму – 3200 грн. Це викликало дискусію в соцмережах. Gazeta.ua пропонує підбірку найцікавіших дописів (Gazeta.ua).

«Звичайно, тут немає ніякого зв'язку. Мінімальний поріг вартості майна, яке вноситься в е-декларацію, – 100 мінімальних зарплат», – написав журналіст Олександр Дубинський.

***

29.10.2016

Свято для народу: як соцмережі реагують на декларації політиків

Електронні декларації, які поспішно заповнюють політики та чиновники першого рангу, викликали великий резонанс у соціальних мережах та ЗМІ (Канал 24).

Політики декларують сотні тисяч доларів, величезні квартири, дорогі авто та різноманітні цінні речі, опис яких викликає подив у виборців.

«24» зібрав підбірку влучних дописів з мережі щодо е-декларування.

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

17.10.2016

Пользовательская база Twitter слабо монетизирована

Twitter имеет серьёзные проблемы с монетизацией базы своих пользователей. В среднем, каждый из них, по отношению к общей капитализации компании, оценивается намного ниже, чем в других соцсетях (HiTech-News.ru).

В Twitter каждый ежемесячный пользователь оценивается, в среднем в 45,11 долларов, тогда как, к примеру, у Facebook этот показатель составляет 216,33 доллара. Если сравнить доходы этих сетей на каждого активного пользователя, то ситуация, опять-таки, не в пользу Twitter (7,99 долларов против 12,96).

В тоже время Twitter имеет отличные возможности для значительного повышения уровня своей монетизации, поскольку эта коммуникационная платформа объединяет в себе огромные ресурсы медиа, социальной сети и мощной базы пользователей. Отличная новостная функция и аналитика абонентов позволяет, по мнению экспертов, видеть хорошие перспективы.

В качестве методов решения текущих проблем Twitter, которыми являются замедление роста абонентской базы и слабая монетизация, компании предлагают задуматься над введением новых сервисов. Таковыми могут стать потоковое видео и трансляция событий (прежде всего политических и спортивных) в режиме онлайн. Эксперты считают, для инвесторов Twitter повышение уровня монетизации компании более выгодно, чем продажа этой соцсети, тем более, что сейчас стоимость её акций заметно упала, до 16,88 долларов за штуку.

В качестве примера для подражания приводится небольшая социальная сеть Angie’s List. Количество её активных пользователей составляет всего 1 % от тех, которых имеет Twitter. Но, при этом, она умудряется зарабатывать на каждом из них по 103 доллара благодаря подписке.

***

17.10.2016

Twitter стоит дешевле своего китайского клона

Американская соцсеть Twitter стала «внезапно» стоить дешевле своего китайского клона Weibo, сообщает Tech In Asia (InternetUA).

Оригинальный сервис микроблогов был основан в 2006 году в США, его «аналог» из КНР существует с 2009 года.

На данный момент рыночная капитализация Weibo составляет $11,35 млрд, рыночная капитализация Twitter – $11,34 млрд.

Как отмечает издание, в настоящее время Twitter находится в состоянии «свободного падения», поскольку ему не удается увеличивать число новых пользователей. За последние 12 месяцев соцсеть теряла 5 млн активных пользователей ежемесячно, на данный момент их число составляет 313 млн.

Weibo, наоборот, продолжает расти. Число пользователей достигает 282 млн, за последний год соцсеть получила 70 млн новых активных пользователей.

***

18.10.2016
«ВКонтакте» приготовила неприятные изменения

Аудиоплеер «ВКонтакте» может начать включать рекламу между песнями. На скрытую возможность в программном коде плеера обратил внимание подписчик паблика Webtackles по имени Алексей Махьянов (InternetUA).

«Скоро в аудизаписях ВК появится реклама», – написал он, приложив к записи скриншот с фрагментом кода.

Администраторы сообщества «Код Дурова», также узнавшие о потенциальной возможности включать рекламу при воспроизведении аудиозаписей, обратились за комментариями к пресс-секретарю соцсети Евгению Красникову.

«После подписания соглашений с музыкальными правообладателями, мы не раз говорили о том, что будем тестировать различные модели монетизации аудиосервиса. Это один из видов тестирования», – рассказал пресс-секретарь «ВКонтакте».

Точная дата внедрения нового формата рекламы остается неизвестной. Напомним, что «ВКонтакте» уже демонстрирует рекламу пользователям, которые смотрят видео – короткие ролики появляются перед основной записью. Так же поступает и популярный видеосервис YouTube.

***

19.10.2016
Сколько зарабатывают звезды в соцсетях

Издание The Economist опубликовало статистику заработков топовых звезд на рекламных постах в своих личных страницах в социальных сетях. Благодаря публикациям селебрити представители различных компаний получают такое взаимодействие с аудиторией, которую не может обеспечить обычная реклама (Телекритика).

Немудрено, что спрос маркетологов на популярные каналы в социальных сетях позволил владельцам страниц с большим количеством подписчиков превратить свой аккаунт в способ зарабатывать существенные денежные суммы.

Так, по подсчетам аналитической платформы Captiv8, больше всего прибыли можно получить с помощью видео на YouTube. Средняя стоимость одной публикации с рекламой на звездном канале с более семи миллионами подписчиков оценивают в 300 тысяч долларов. Пост на странице в Facebook с аналогичным количеством фанов приносит селебрити свыше 187 тысяч долларов за пост. Одно фото или видео в Instagram и Snapchat с таким же количеством подписчиков будет стоить по 150 тысяч долларов, в Vine – более 112 тысяч долларов и 60 тысяч – за твит в Twitter.

***

20.10.2016
«ВКонтакте» создаст мобильного оператора – СМИ

Российская социальная сеть «ВКонтакте» до конца года запустит собственный виртуальный оператор сотовой связи – Vkmobile, пишут «Известия». Оплачивать услуги можно будет как деньгами, так и специальными действиями, например просмотрами рекламы и ее перепостами (Четверта Влада).

О планах «ВК» создать оператора изданию рассказал источник, близкий к руководству компании. По его словам, оператор будет работать под брендом VKmobile, его запуск может состояться до конца этого года. Переговоры об аренде сетевой инфраструктуры уже проведены с «МегаФоном». Для сайта оператора зарегистрирован домен VKmobile.me.

Представители ВКонтакте и МегаФона от комментариев воздержались.

Собеседник издания сообщил, что за услуги связи VKmobile можно будет расплачиваться как деньгами, так и определенными действиями. Такая модель бизнеса называется «фримиум» (от английских слов free – бесплатный и premium – премиальный): за услуги связи пользователям можно будет лайкнуть рекламный пост, вступить в определенную группу, чем-то поделиться, что-то посмотреть и прочее.

Согласно данным статистики Liveinternet, среднесуточная посещаемость сайта «ВКонтакте» составляет порядка 80 млн человек. По данным TMT Консалтинг, самая большая абонентская база сегодня у МТС – 77 млн, у МегаФона – 75 млн, у ВымпелКома (бренд Билайн) – 58 млн и у Т2 РТК Холдинг (бренд Tele2) – 38 млн.

***

19.10.2016
Втома від додатків: що може прийти на зміну програмам

Користувачі втомилися від мобільних додатків, експерти вже замислюються над тим, що може прийти на зміну звичним програмам (Espreso.tv).

Про це пише Tech Today з посиланням на BBC.

Один із головних кандидатів на заміну – боти. Це програми, які працюють на віддалених серверах, більше відомих сьогодні як «хмари». Доступ до таких утиліт можна отримувати через Інтернет, а завдяки штучному інтелекту робота з ними нагадує спілкування. Сьогодні боти використовуються все більше – на сайтах магазинів, служб таксі та доставки, в чатах та месенджерах.

Чому боти

Попри мільйони доступних утиліт у маркетах програм у середньому ми використовуємо 27 утиліт, за даними аналітиків компанії Nielsen. І ця цифра не змінюється з роками. Ще одна проблема з додатками – нескінченний потік оновлень. Так, сьогодні це стало модно, і кожен хоче оновлюватися якомога більше. Але апдейти часто несуть нові проблеми, споживають місце на диску, більш вимогливі до процесорної потужності тощо.

«Одна з найгірших речей у App Store – це сам App Store. Це сильно огороджений садок», – говорить програміст Тед Неш. За його словами, керівництво Apple сповільнює розробку програм. Компанія також змушує програмістів включати у свої додатки спеціальний код, який стежить за рекламою, статистикою використання та іншими метриками. До цього, говорить він, треба ще додати складність адаптації утиліт під різні платформи.

Радість тексту

Боти можуть принести полегшення ситуації, що склалася. «Додатки були класною річчю, – говорить голова відділу мобільних розробок компанії Sage Кріті Шарма Sage. – Але все більше людей спілкується в месенджерах, аніж залишає пости в соцмережах». Ось чому вона вважає ботів природним наступником додатків – інтерфейс перших уже буде знайомий користувачам.

За словами Шарми, месенджери дозволили користувачам освоїтися з текстовими розмовами. Для компаній та брендів, які хочуть плідної взаємодії з клієнтами, використання ботів може забезпечити такі розмови. Компанія Sage, де працює Шарма, розробляє бота на ім’я Pegg, який може слугувати «розумним» бізнес-асистентом. Він допоможе власникам малого бізнесу стежити за витратами та прибутком. «Боти не повинні бути суперскладними, – говорить вона. – Але з часом вони мусять стати ціннішими для користувачів».

Переваги ботів

Боти стають популярними завдяки прогресу в розробці програм на основі штучного інтелекту. А також завдяки тому, що компанії сьогодні мають величезні масиви даних, на яких вони тренують ботів.

Інша перевага ботів над додатками – швидкість їхньої розробки, розгортання та оновлення. Адже вони працюють на одному сервері, який контролює компанія.

Інтерес до ботів також підігріває увага таких гігантів, як Facebook, Microsoft та Google. До них також звертаються невеликі фірми, серед яких Slack, HipChat, Begin, Growbot, Butter, Wisdom, Operator. Наприклад, Facebook цього року оголосила про запуск фреймворку для ботів, який спростить їхню розробку.

За оцінками експертів, цікавість до ботів з боку інвесторів дорівнює близько $4 млрд. «Боти – це новий чорний (мається на увазі чорний колір як один з найпопулярніших кольорів – ред.)», – говорить директор з продукції сервісу бронювання залізничних квитків Trainline Джон Мур. Сьогодні більшість клієнтів цієї служби користується спеціалізованим мобільним додатком, але фірма вивчає можливості ботів.

Трохи скептики

Не всі переконані, що боти відразу замінять додатки. «Бот з точки зору користувача є набагато простішим. Але штучний інтелект, який забезпечує його роботу, насправді дуже складний, – говорить розробник Тед Неш з компанії Tapdaq. – Багато з них зараз мають готові вводи та відповіді. Вони стануть по-справжньому популярними, лише коли відповідатимуть так само, як люди».

***

30.10.2016
LinkedIn вернулась к прибыли впервые за год

Деловая социальная сеть LinkedIn, которая в скором времени войдет в состав Microsoft, отчиталась о результатах деятельности в третьем квартале. Впервые более чем за год компания вернулась к прибыли. (InternetUA).

В июле-сентябре 2016 года чистая прибыль LinkedIn составила 8,6 млн долларов против убытка в размере 47,4 млн долларов годом ранее. Три предыдущих квартала также были убыточными для сервиса. Выручка компании увеличилась на 23 % в годовом исчислении, достигнув 959,7 млн долларов.

По итогам третьей четверти 2016 года на продаже премиум-аккаунтов LinkedIn заработала 162 млн долларов, что на 17 % больше показателя годичной давности. Рекламный бизнес, за который отвечает подразделение Marketing Solutions, показал 26-процентный прирост выручки – до 175 млн долларов. Сервис платных объявлений работодателей и соискателей вакансий принес компании доход в 623 млн долларов (+24 %).

За год общее количество пользователей LinkedIn увеличилось на 18 %, до 467 млн. Число уникальных посетителей сервиса в месяц повысилось на 9 %, до 106 млн, а просмотр страниц возрос на 27 %.

В середине июня 2016 года Microsoft объявила о приобретении LinkedIn за 26,2 млрд долларов. Сделку планируется закрыть до конца года.

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

18.10.2016
Сергей Бражник
Адепты подростковых суицидов засветились в Харькове

Салтовская детвора попала под угрозу ("Город Х").

Настораживающая надпись появилась на двери подъезда девятиэтажки по ул. Гарибальди, 11.

Ничего не значащую с первого взгляда фразу «киты погибают в лужах бензина» написали синим фломастером на металлической поверхности. Мало кто знает: различные выражения с умирающими китами ведут в интернет-группы, где подростков прямо или косвенно призывают к самоубийствам.

Так, в соцсетях существует несколько сообществ «Киты умирают в лужах бензина». Самое крупное из них насчитывает почти 21 500 участников (более сотни из них – харьковские подростки). Есть и более мелкие аналогичные группы, но наполнение везде схоже – депрессивные цитаты, стихи и картинки.

О пабликах, которые склоняют детей к суициду, «ГХ» уже писал более подробно. Там все начинается с погибающих китов – детей заманивают в сообщества, провоцируют на разговор в личных сообщениях, предлагают пройти специфические квесты, которые дают доступ к закрытым группам. Именно там и происходят самые жуткие вещи – ребятам буквально дают ЦУ о том, как лишить себя жизни. Впрочем, ранее харьковские правоохранители не связывали подростковые самоубийства в нашем городе с группами в соцсетях.

***

24.10.2016

Instagram окажет психологическую поддержку пользователям склонным к суициду

Социально ориентированные сервисы предоставляют людям удобную возможность поделиться своими сокровенными мыслями с окружающими. При этом некоторые используют соцсети, чтобы рассказать о своих проблемах или отчаянии, которое иногда подталкивает к совершению необдуманных поступков. Для своевременной фиксации резкой смены настроения у пользователей фотосервиса Instagram, разработчики внедрят специальный инструмент, способный уведомлять о настораживающих сообщениях, связанных с суицидальными темами (IGate).

Активировать такую себе «тревожную кнопку» сможет каждый пользователь, обративший внимание на намеки в сообщении причинить вред самому себе. После проверки администрация Instagram, отправит автору поста послание с предложением помощи:

«Кто-то прочитал написанную вами запись и полагает, что сейчас вы переживаете трудный период в жизни. Если вам необходима поддержка, мы хотели бы ее предоставить».

В случае проявленного интереса, пользователю предложат позвонить на горячую линию, где будет предоставлена квалифицированную помощь, а также воспользоваться услугами специальных сайтов.

***

30.10.2016

Просмотр чужих «селфи» может нанести удар по самооценке

Чувствуете себя подавленным и разочарованным? Новое исследование ученых из Школы коммуникаций Пенсильванского государственного университета свидетельствует о том, что винить в этом следует самого себя, и «селфи». (InternetUA).

Частый просмотр «селфи», автопортретов, сделанных с помощью смартфона или цифровой камеры и размещенных на различных сайтах, а также в социальных сетях, таких как Facebook, связан со снижением самооценки и степени удовлетворенности жизнью, выяснили авторы исследования.

«Изобретение» термина «селфи» приписывают одному пьяному австралийскому студенту, который в 2002 году опубликовал свою фотографию с разбитыми опухшими губами, после того как он упал во время вечеринки по случаю 21-го дня рождения своего друга. Тем не менее, большинство людей, как правило, размещают селфи, где они изображены счастливыми и веселыми, и, да, порой пьяными.

У человека, часто рассматривающего фотографии знакомых с улыбающимися лицами и невероятными гримасами, может возникнуть вопрос, почему он сам не проводит время так же хорошо и весело, как эти люди.

А это может привести к снижению самооценки и удовлетворенности жизнью, утверждает Руоксу Ван, ведущий автор работы под названием «Исследование психологических эффектов размещения и просмотра одиночных и групповых портретов в социальных сетях». «Речь идет о классическом психологическом феномене под названием «социальное сравнение снизу вверх», считает этот аспирант по специальности «массовые коммуникации».

Исследование, результаты которого были опубликованы в онлайн-версии Journal of Telematics and Informatics, показало, что, напротив, частый просмотр групповых портретов, или «групи», приводит к росту самооценки и удовлетворенности жизнью.

«Вероятно, это связано с тем, что когда люди рассматривают „групи“ в социальных сетях, они испытывают чувство общности, которое может содержаться в самих групповых снимках, которые они видят». К такому выводу привело исследование, проведенное путем онлайн-опроса среди 275 участников в Соединенных Штатах.

Кроме того, исследователи обнаружили, что еще больший положительный эффект просмотр «селфи» и «групи» производит на тех людей, которые остро ощущают необходимость в популярности, вероятно, в связи с тем, что такой просмотр удовлетворяет их желания.

«Изначально мы предполагали, что на самооценку может оказывать влияние размещение селфи в социальных сетях, но в ходе исследования было обнаружено, что именно просмотр этих фотографий, а не их размещение, производит этот эффект», сказал Ван, чьими соавторами были аспирант Фань Ян и доцент Мишель Хейг.

Ученые были крайне удивлены, узнав, что размещение в социальных сетях «селфи» и «групи» не произвело значительных психологических эффектов на участников исследования.

«В результате нашего исследования мы пришли к выводу, что когда человек размещает фотографии в социальных сетях, он должен понимать, что его действия оказывают психологическое воздействие на других людей», – заключил Ван.

***

29.10.2016

Як Facebook викриває наші особисті таємниці

Наші пости і статуси в соціальних мережах розповідають про нашу особистість набагато більше, ніж ми вважаємо, зазначає bbc.com (Рідний Київ).

«Що у вас на думці?» питає Facebook щодня 1,7 мільярдів своїх активних користувачів. Таке саме питання ставлять своїм клієнтам на початку сеансу психотерапевти, психологи та консультанти. І те саме запитуємо ми в близької людини, якщо вона виглядає стурбованою.

Наша поведінка в соціальних мережах на подив точно віддзеркалює наш психологічний стан, і відбувається це зазвичай ненавмисно. Не дивно, що психологи, які намагаються зрозуміти емоційний стан окремої людини, спільноти або навіть цілої нації, вже давно почали звертати увагу на ці підсвідомі сигнали.

Психологія нашої поведінки в соцмережах – це одна з тем, яку обговорюватимуть на саміті BBC Future «Ідеї, які змінюють світ». Конференція відбудеться в Сіднеї в листопаді цього року.

Що розповідають про мене мої пости в соцмережах?

Типи повідомлень і те, як часто ми постимо їх, розповідають набагато більше про нашу особистість і наш емоційний стан, ніж зміст самих дописів.

Дослідження, в якому взяли участь 555 користувачів Facebook в США, виявило, що екстраверти зазвичай пишуть у мережі про свою соціальну активність і повсякденне життя та роблять це досить часто.

Люди з низькою самооцінкою, як правило, розповідають про свого романтичного партнера. Невротики шукають засобів переконатися в своїй цінності або привернути увагу. А нарциси постійно хваляться досягненнями або співають дифірамби своїй дієті та спортивному режиму.

Інше дослідження показало, що люди, які невпинно постять селфі, самозакохані і схильні до психопатії. А ті, хто обробляє свої фотографії, перш ніж запостити їх в соціальні мережі, вочевидь, має низьку самооцінку.

Соцмережі – як психотерапевт?

Напевно, вам відоме те полегшення, яке відчуваєш, написавши гнівну тираду в Facebook або запостивши сумний твіт о третій ночі. Доволі часто ми користуємось соціальними мережами, як своїм власним психотерапевтом.

Але чи допомагає насправді цей плач у порожнечу? Можливо, він лише погіршує наші проблеми?

Дослідники Центру психічного здоров'я та гендерних проблем в Мехіко погоджуються з цим. Вони запустили соціальну кампанію, яка попереджає громадян про те, що Facebook не може замінити належну психологічну допомогу.

Утім, порожнеча має вуха. Дослідники шукають способи відстежувати статуси або повідомлення в Twitter, які можуть вказувати на суїцидні настрої користувачів.

Австралійський інститут Black Dog, який є світовим лідером у дослідженні психічних розладів, упродовж двох місяців проводив експеримент. За допомогою комп'ютерної програми дослідники відстежували у твітах користувачів фрази та окремі слова, які могли вказувати на наміри скоїти самогубство.

За допомогою програми дослідники змогли виявити тривожні дописи. Цікаво, що результати, отримані комп'ютером, і висновки дослідників практично збігались. Це означає, що вже незабаром, комп'ютерна програма зможе визначати користувачів, які потребують негайної допомоги, і повідомляти про них лікарям чи родичам.

Деякі інтернет-спільноти також визнають, що вчасно визначати суїцидні статуси користувачів, є дуже важливим. Вони організують свої власні мережі психологічної підтримки.

Наприклад, користувачі соціальної мережі Reddit створили спеціальну сторінку Suicide Watch, на якій члени спільноти можуть висловитися і підтримати тих, хто потребує психологічної допомоги.

І хоча тролінг є неминучим явищем на подібних форумах, багато коментарів демонструють щире бажання допомогти людині пережити біль.

Небажання спілкуватись у соціальних мережах також може свідчити про проблеми психологічного характеру. В одному дослідженні вчені за допомогою зв'язаного з Bluetooth додатку визначали моделі онлайн-поведінки молодих людей. Коли користувачі менше спілкувались зі своїми друзями в соцмережах або видаляли свої акаунти, це в багатьох випадках було ознакою депресії.

Емоційний настрій нації?

Представники окремих спільнот, цілих націй і навіть людство взагалі зазвичай разом переживають злети і падіння. Інститут Black Dog і австралійська наукова агенція CSIRO вирішили виміряти емоційний пульс всієї планети.

В рамках проекту «We Feel» дослідники спостерігають за емоціями користувачів в соціальній мережі Twitter. Вони також випадково обирають 1% публічних твітів, аналізуючи в середньому 19 тисяч повідомлень щохвилини, щоби визначити загальний психологічний настрій мережі в певний момент часу.

Результатом цього є мапа емоцій, яка демонструє у відсотковому відношенні різні емоційні стани спільноти – подив, радість, любов, печаль, гнів

або страх – в різних частинах світу. Мапа віддзеркалює реакцію спільноти на різні національні та глобальні події.

Дослідники також проаналізували повідомлення в Twitter за допомогою онлайн-інструменту, який вимірює рівень «позитивності» різних мов, зокрема англійської, французької, арабської та індонезійської.

За допомогою «гедонометру» дослідники проаналізували повідомлення в Twitter, статті в онлайн виданнях, книги Google і навіть назви кінофільмів і визначили 10 тисяч найпоширеніших слів в кожній мові. Потім вони попросили носіїв мови оцінити кожне слово за шкалою позитивності-негативності.

Аналіз показав, що в цілому позитивні соціальні емоції переважають в усіх мовах, хоча перше місце в рейтингу з великим відривом посіли іспанська і португальська.

Тепер за допомогою цього інструменту дослідники виміряють середній рівень щастя в користувачів Twitter. Вони вже з'ясували, як певні події впливають на настрій користувачів мережі.

Дебати навколо виборів президента США, приміром, знижують рівень позитивних емоцій, так само як і розлучення Джолі і Пітта, а от легалізація одностатевих шлюбів, навпаки, покращила настрій спільноти.

Дослідники також намагаються з'ясувати, як задоволення життям співвідноситься з іншими чинниками, зокрема соціально-економічним статусом, місцем проживання і демографічними показниками в різних частинах США.

Отже, коли наступного разу ви зберетеся написати щось у соціальній мережі, подумайте про те, що ваш допис чимало розповість про ваші думки, настрій і психологічний стан.

Можливо, набагато більше, ніж ви насправді хотіли відкрити світу.

Маніпулятивні технології

18.10.2016

ЕС создает бюро по противодействию российской пропаганде (El Pais, Испания)

Люсия Абельян, корреспондент в Брюсселе

Брюссель издает так называемые «дезинформационные журналы», чтобы опровергнуть кремлевские утверждения (Четверта Влада).

«Будь внимателен к тому, что потребляешь», предупреждает видеоролик, который в течение чуть более двух минут преподносит российскую пропаганду, как опасное для здоровья блюдо. Снятый в коричневых тонах, со звуковым фоном на русском и английском языках, этот ролик не является произведением какого-нибудь антироссийского блогера или прозападного мозгового центра.

Его автором является сам Евросоюз, решивший противостоять российской дезинформации при помощи альтернативных аргументов. Это небольшое бюро при европейской дипломатической службе пытается разрушить распространяемые Кремлем мифы о ЕС. «Это битва Давида с Голиафом. Но я не хочу быть излишне пессимистичным», – рассказывает источник в ЕС, который знает, что из себя представляет данное бюро, называющееся «Стратегией распространения информации ЕС на восточном направлении».

Плоды этого проекта с начала года можно посмотреть на сайте euvsdisinfo.eu. Источники, предпочитающие оставаться неизвестными, указывают на то, что цель указана в самом названии сайта: ЕС против дезинформации. Но также признают, что инициатива призвана идти дальше исправления обнаруженных ошибок и давать положительные сведения о Европе.

Всего лишь за 10 месяцев своей работы бюро еженедельно отправляло напрямую информацию более чем 18 тысячам русскоговорящих людей, проживающих как в самой России, так и в граничащих с ней на востоке странах. Чтобы завоевать привлекательность среди читателей (журналистов, исследователей и т.д.), эксперты ЕС еженедельно разрабатывают привлекающие внимание материалы: по вторникам они выпускают так называемый журнал дезинформации, а по пятницам – обзор дезинформации, в который они включают пятничную шутку. Например, 14 октября в ней речь шла о мнимом опросе, согласно результатам которого российский президент Владимир Путин стал самым популярным кандидатом среди американцев, оставив позади Хиллари Клинтон и Дональда Трампа. «Должны ли мы испытывать беспокойство в связи с тем, что в комментариях к новости говорится, что количество перепостов (911) является неким знаком?», иронично задается вопросом автор заметки, чье имя, как и всех прочих авторов, не называется.

Чтобы не привлекать лишнего внимания, бюро работает, не имея собственного бюджета и штатных сотрудников. Оно подчиняется аудиовизуальной службе Европейского Совета и другим структурам дипломатической службы. Количество постоянных сотрудников – это чуть больше десяти человек, которым помогают дипломаты стран ЕС и 450 информаторов (журналистов, экспертов и ученых, работающих на добровольных началах), находящиеся в районах российского влияния и предупреждающих о распространяемой Кремлем лжи. В среднесрочной перспективе бюро рассчитывает расширить свою деятельность.

В соцсетях бюро публикует свои материалы под тем же самым именем: euvsdisinfo. У него уже более 13 тысяч подписчиков в Twitter и Facebook. Каждый месяц проводится оценка эффективности работы. В качестве примера того интереса, который вызывает ЕС среди русскоговорящего населения, источники привели переведенное на русский язык заявление Высокого представителя ЕС по вопросам внешней политики Федерики Могерини (Federica Mogherini), в котором она осуждает аннексию украинского

полуострова Крым в марте 2014 года, собравшее рекордное количество просмотров. После появления русскоязычной версии сайта она стала второй по посещаемости после англоязычной.

В сердце Европы

Несмотря на эти достижения, эффективность данной контрпропаганды весьма ограниченна. По другую сторону барьера действуют крупные российские СМИ, которые тратят на эти цели как минимум миллиард евро и распространяют свои материалы во всех соседних странах, расположенных к востоку от России (в частности, на Украине, в Грузии и Молдавии), в самом Евросоюзе – в странах Прибалтики, Восточной Европы и все более интенсивно в самом сердце Европы.

Главная задача сейчас заключается в том, чтобы нейтрализовать этот вызов. Специалисты в области российской политики заявляют, что в целом ряде европейских эпизодов пропагандистское давление значительно возросло. Во-первых, произошедшая два года назад катастрофа лайнера Малазийских авиалиний, который следовал из Амстердама и был сбит во время пролета над восточной частью Украины. Официальное расследование пришло к выводу о том, что ракета, сбившая самолет, была доставлена из России, однако Москва это отрицает.

Еще большую тревогу вызвал резонанс, вызванный в Германии случаем с русской 13-летней девочкой, заявившей, что ее изнасиловали несколько мигрантов. Раздутый российскими СМИ случай оказался фальшивкой, однако в обстановке кризиса с беженцами сумел вызвать смятение. Но бюро контрпропаганды старается работать на опережение. «Чего ждать еще? Мы видели сюжет про избирательные бюллетени в США. Возможно для того, чтобы обвинить Хиллари Клинтон в попытке присвоить себе голоса избирателей», считают источники, к которым мы обратились.

***

27.10.2016

В Днепре СБУ задержала администратора антиукраинских групп в соцсетях

Сотрудники Службы безопасности Украины задержали в Днепре местного жителя, который вел активную антиукраинскую пропаганду в социальных сетях (МОСТ-ДНЕПР).

Об этом ИА «МОСТ-ДНЕПР» сообщили в пресс-службе СБУ.

Правоохранители установили, что мужчина, который принимал участие в пророссийских акциях, в 2014 году стал администратором нескольких групп антиукраинской направленности. Он через Интернет познакомился с представителями спецслужб РФ и согласился распространять сепаратистские материалы на различных информационно-политических пабликах в российских соцсетях.

Информация для публикаций излагалась в специально созданном «закрытой» сообществе. По указанию своих кураторов, злоумышленник распространял информацию, направленную на дискредитацию украинского государства и армии, разжигание межнациональной розни, введение русского языка как государственного, а также пропагандировал выход Днепропетровской области из состава Украины и вхождение в состав Российской Федерации.

Во время обыска сотрудники спецслужбы изъяли у злоумышленника компьютерную технику с доказательствами антиукраинской деятельности», – отмечает пресс-служба.

Открыто уголовное производство по ч. 2 ст. 110 Уголовного кодекса Украины. Продолжаются оперативно-следственные действия.

***

26.10.2016

СБУ затримала поборницю «Сумської народної республіки»

Служба безпеки України затримала пропагандистку «русского мира», яка активно поширювала в соціальній мережі російського походження антиукраїнські матеріали і закликала до створення т. зв. «Сумської народної республіки» (LB.ua).

Про це інформує прес-центр СБУ.

«Непрацююча жителька обласного центру влітку цього року погодилася на пропозицію представників терористичної організації „ДНР/ЛНР“ за гроші поширювати матеріали, які дискредитують державну владу України, популяризують ідеї сепаратизму, а також закликають до активних дій з приєднання Сумської області до т. з. „Новоросії“», – йдеться в повідомленні.

Відкрито кримінальне провадження з ч.1 ст.110 (посягання на територіальну цілісність і недоторканність України) Кримінального кодексу України.

Раніше в жовтні СБУ знайшла квазіреспубліку в Чернігівській області.

***

22.10.2016

Німецькі партії дискутують про застосування ботів у соцмережах

Правопопулістська партія «Альтернатива для Німеччини» визнала, що використовуватиме ботів у соцмережах під час передвиборчої кампанії (DW.com).

У Німеччині розгорілися дебати стосовно використання ботів у соцмережах у політичній боротьбі. Приводом стала заява правопопулістської партії «Альтернатива для Німеччини» (АдН) про наміри використовувати ботів у ході передвиборчої кампанії наступного року. «Само собою зрозуміло, ми включимо соціальних ботів у нашу стратегію на виборах до Бундестагу, –

зауважила представниця правління АдН Аліс Вайдель в інтерв'ю виданню Spiegel. – Саме для таких молодих партій, як наша, засоби соціальних мереж є важливими інструментами поширення нашої позиції серед виборців».

Парламентські партії різко відреагували на такі слова. «Соціальні медіа гратимуть важливу роль для нас у передвиборчій боротьбі, але ми відкидаємо використання ботів», – проголосила генеральна секретарка Соціал-демократичної партії Німеччини Катаріна Барлі. «Це показує, АдН не йдеться про справжню змістовну дискусію – тільки про безладдя та провокації», – зазначив генеральний секретар Християнсько-демократичного союзу Петер Таубер.

Ліва партія закликала відмовитися від застосування ботів у соцмережах під час виборів. «Боти в соцмережах можуть становити загрозу демократії», – заявив у суботу, 22 жовтня, представник правління Лівої партії Маттіас Ген. Зелені також висловилися проти використання ботів у передвиборчій кампанії.

Боти у соцмережах на кшталт Twitter або Facebook – це програми, які продукують коментарі певного змісту. Таким чином політичні сили поширюють ілюзію суспільного інтересу до певних тем та ідей. Згідно з дослідженням Оксфордського університету, боти в соцмережах широко застосовуються. Так, після перших дебатів між кандидатами у президенти США Дональдом Трампом і Гілларі Клінтон більше, ніж кожен третій твіт на підтримку Трампа був написаний ботом (37 відсотків). У Клінтон цей показник – 22 відсотки.

Зарубіжні спецслужби і технології «соціального контролю»

17.10.2016
Найден способ обезопасить пользователей Tor от деанонимизации

Спецслужбы и правоохранительные органы продолжают инвестировать средства в исследования, связанные с деанонимизацией пользователей сети Tor. Поскольку правительство не намерено раскрывать эксплуатируемые им уязвимости, команды Tor Project и Mozilla Firefox (браузер Tor создан на базе Firefox) объединились в работе над улучшением безопасности анонимайзера (InternetUA).

Целью улучшений является сделать невозможным для вредоносного ПО собирать информацию, позволяющую раскрыть личность пользователя. Изменив то, как браузер подключается к сети, разработчики сильно усложнят задачу для вредоносного ПО.

«На данном этапе у нас уже есть базовые инструменты, и мы работаем над их объединением с целью определить их эффективность в обеспечении безопасности», – сообщил журналистам Motherboard эксперт Mozilla Ричард Барнес (Richard Barnes).

Как пояснил Барнес, браузер Tor состоит из двух частей – модифицированной версии Firefox и прокси, направляющего трафик браузера в сеть Tor. У первой части (Firefox) также есть доступ к сети, поскольку ей нужно обращаться к прокси. «То есть, если атакующему удастся скомпрометировать Firefox, он сможет деанонимизировать пользователя, подключив браузер не к Tor, а к чему-то другому», – сообщил Барнес.

Именно такой метод использовало ФБР в ходе расследований, связанных с подпольными сайтами даркнета. В феврале 2015 года бюро применило так называемую «технику исследования сети» («network investigative technique» или NIT), являющуюся ничем иным, как вредоносной программой. ПО эксплуатировало уязвимость в браузере Tor, и в результате компьютер подключался к подконтрольному ФБР серверу, находящемуся за пределами анонимной сети. Таким образом следователям удалось выяснить настоящие IP-адреса подозреваемых.

NIT станет бесполезной, когда разработчики добавят поддержку сокетов домена UNIX (UDS) и другие нововведения. UDS позволяет двум разным программам на одном компьютере взаимодействовать между собой без необходимости использовать сетевой протокол передачи данных. Благодаря UDS браузеру Firefox и Tor больше не нужен будет доступ к сети.

«Это значит, что вы сможете запустить его (браузер – ред.) в песочнице без доступа к сети (только с сокетом домена UNIX), и он все равно будет работать. Даже если Firefox будет скомпрометирован, установить соединение, позволяющее деанонимизировать пользователя, будет невозможно», - отметил Барнес.

***

19.10.2016

МВС Росії створило робота для перевірки публікацій на екстремізм

МВС Росії представило новий технологічний проект, призначений для автоматизації досліджень матеріалів екстремістської спрямованості (LB.ua).

Апаратно-програмний комплекс «Фоб» є комп'ютерним комплексом, оснащеним інформаційно-пошуковою системою екстремістських матеріалів, передає РИА Новости.

«Цей комплекс дозволяє автоматизувати складні дослідження, в тому числі знаходити дублікати раніше досліджених зображень, ототожнювати символи, перевіряти відео за стоп-кадрами, якщо раніше таке вже було визнане екстремістським. У тому числі якщо в зображенні використана текстова фраза-символ, яку часто застосовують з екстремістською метою, то експерт може в пошуковій системі виявити аналоги», – розповів поліцейський експерт, який демонстрував новинку експертно-криміналістичного центру МВС Росії на XX міжнародній виставці засобів забезпечення безпеки «Інтерполітех 2016».

«Фоб» розроблено для дослідження матеріалів з поєднанням вербальних, візуальних і аудіокодів, що дозволяє оперативно виявити матеріал з ознаками екстремізму і подати на аналіз експертам.

***

18.10.2016

Таиланд призвал Facebook и YouTube заблокировать оскорбительные для монархии страницы

Таиланд ужесточает борьбу с критикой в адрес высокопоставленных представителей королевской семьи, сообщает Bloomberg. Это происходит после смерти короля Пхумипона Адульядета (InternetUA).

В частности, местным офисам компаний Facebook, Twitter, YouTube и Line были направлены письма с просьбой заблокировать доступ к страницам, признанным оскорбительными для монархии.

Мониторингом трансляций по радио и телевидению, а также в соцсетях будет заниматься специальная команда.

Признанным виновными в клевете, оскорблении или нанесении угроз в адрес короля, королевы, наследника или регента грозит до 15 лет тюрьмы.

***

21.10.2016

США може довести причетність Росії до хакерських атак

Спецслужби США мають докази причетності Росії до хакерських атак на сервери американських політичних організацій, заявив директор Національної розвідки США Джеймс Клеппер на брифінгу. Про це повідомляє Wall Street Journal (Корреспондент.net).

«Я не збираюся обговорювати основну доказову базу для такої заяви. Коли ми говоримо, що впевнені, думаю, це говорить само за себе», – наголосив Клеппер.

Він також зазначив «непохитну впевненість» вищих осіб США в тому, що за атаками стоїть Росія.

***

26.10.2016

В России могут заблокировать известную соцсеть

В Российской Федерации собираются заблокировать социальную сеть для поиска работы LinkedIn, заявив, что она нарушает требования российских законов закона о хранении персональных данных граждан страны в России (InternetUA).

Об этом пишет Русская служба BBC.

Решения о блокировании соцсети роскомнадзор будет добиваться в Мосгорсуде.

Отмечается, что в августе Роскомнадзор обратился в Таганский суд Москвы после того, как не получил от соцсети ответов на два запроса с просьбой предоставить информацию об исполнении закона о персональных данных.

В итоге суд удовлетворил иск о блокировке сайта.

«Если Мосгорсуд подтвердит решение суда первой инстанции, мы внесем соцсеть в реестр нарушителей персональных данных, что предполагает блокировку ресурса на территории России», – рассказали в пресс-службе ведомства.

По словам пресс-секретаря Роскомнадзора Вадима Ампелонского ведомство воспользовалось «правом обращения в суд в полном соответствии с алгоритмом взаимодействия с иностранными компаниями, которые не имеют представительства в России».

Он рассказал, что LinkedIn подал в Мосгорсуд апелляцию на решение Таганского суда, в минувшую субботу заседание перенесли на 10 ноября.

Российский закон о персональных данных обязывает хранить личные данные россиян на территории РФ.

***

29.10.2016

Развивающиеся страны теряют миллиарды из-за правительственных блокировок приложений

За последний год развивающиеся страны потеряли $2,4 млрд ВВП из-за того, что их власти отключали всему населению интернет или блокировали отдельные приложения. Причинами отключения служили массовые волнения, экзамены, национальные праздники и нечестная конкуренция (InternetUA).

Развивающиеся страны потеряли более $2,4 млрд валового внутреннего продукта (ВВП) в связи с правительственными отключениями всего интернета или отдельных ресурсов за последний год. К такому выводу пришли исследователи Брукингского института в США, проанализировавшие блокировку сети или различных сайтов и приложений на общенациональном уровне в 19 странах. Исследуемый период – с 1 июля 2015 г. по 30 июня 2016 г.

Больше всего пострадала Индия, где правительство лишило граждан интернета или его отдельных ресурсов примерно на 79,54 суток за весь год. За это время страна успела потерять более $968 млн ВВП. На втором месте Саудовская Аравия, где блокировки длились в сумме 45 дней, что обошлось государству более чем в $465 млн ВВП. Третье место занимает Марокко, где различные ресурсы сети были недоступна 182 дня в год, при этом страна потеряла порядка $320 млн ВВП.

Количество блокировок

В 19 рассмотренных странах был отмечен 81 случай правительственного отключения интернета или блокировки отдельных ресурсов. Из них 36 инцидентов – это отключение интернета во всей стране, 17 – в отдельном регионе страны.

Также был зарегистрирован 1 случай отключения мобильной связи во всем государстве, 22 случая – в отдельном регионе. Кроме того, было отмечено 14 случаев общенациональной блокировки различных приложений, чаще всего – мессенджеров и соцсетей.

Самые резонансные случаи

В мае 2015 г. Саудовская Аравия заблокировала ряд мессенджеров, в том числе WhatsApp, Facebook Messenger и Skype, объяснив это тем, что они не отвечали местным телекоммуникационным регулировкам. В качестве неофициальной причины называют жалобы мобильных операторов, которые теряют прибыль с распространением голосовых звонков по интернету. Во время этой акции страна потеряла $465 млн ВВП.

По аналогичным причинам в Марокко с 1 января 2016 г. были заблокированы Skype, Viber, Tango, WhatsApp и Facebook Messenger, что обошлось государству в $320 млн ВВП.

В феврале 2016 г. Индия на неделю заблокировала все мобильные сервисы в районе городов Ротхак и Джаджар в связи с масштабными акциями протеста. Это лишило страну $190 млн ВВП.

Кроме того, Индия применила в 2015 г. практику, позаимствованную у Алжира и Ирака, – в стране начали отключать интернет во время проведения особо важных экзаменов. Доступ к сети невозможен в дни экзаменов с 9:00 до 13:00, чтобы школьники и студенты «не могли использовать свои смартфоны не по назначению», поясняют власти.

В течение 2015 г. суд Бразилии несколько раз блокировал WhatsApp, поскольку правоохранительные органы страны пытались получить от компании доступ к данным пользователей. Отключение WhatsApp по всей стране на один день в мае месяце привело к потере $39 млн ВВП.

Другие инциденты

В 2015 г. Пакистан частично отключил интернет и мобильную связь в Исламабаде в период с 12 по 23 марта в связи с празднованием Дня Пакистана. Операторам было отдано распоряжение не предоставлять услуги в радиусе 5 км от места проведения общенационального парада. В эту зону попали аэропорт, крупный госпиталь и офисы многих компаний.

Весной 2015 г. африканское государство Бурунди заблокировало WhatsApp и Viber, чтобы помешать участникам политических протестов общаться между собой. Протесты граждан были вызваны выдвижением президента Пьера Нкурунзизы на третий срок.

Осенью 2015 г. Турция заблокировала Twitter и Facebook, чтобы пользователи не могли распространять фотографии с места теракта в Анкаре, где 10 октября в результате двух взрывов во время массовой акции погибло более 100 человек. По словам властей, распространение фото сеяло панику

среди населения. Блокировка некоторых соцсетей является в Турции обычной мерой борьбы с последствиями терактов.

Интернет и национальный ВВП

В ходе исследования сотрудники Брукингского института подсчитали, какой процент ВВП зависит от интернета в различных странах, в том числе в развитых. На первой строке списка оказалась Великобритания, которая получает от онлайн-деятельности 12,4 % ВВП. На втором месте Южная Корея (8 % ВВП), на третьем – Китай (6,9 % ВВП). Далее идут Индия (5,6 % ВВП), Япония (5,6 % ВВП) и США (5,4 % ВВП).

Проблема захисту даних. DDOS та вірусні атаки

18.10.2016
4 неочевидных способа слежки за вами

Современные мобильные устройства имеют огромное количество датчиков, сенсоров и прочих комплектующих внутри корпуса. Многие даже не подозревают, что злоумышленники могут прослушивать через гироскоп или отследить местоположение по аккумулятору, сообщает «Медуза» (InternetUA).

Прослушка с помощью гироскопа

Группа исследователей из Америки и Израиля продемонстрировала, как датчик ориентации в пространстве, который есть почти во всех современных смартфонах, можно использовать для прослушки. Дело в том, что гироскоп состоит из очень чувствительных сенсоров, состоящих из вибрирующей пластины и чипа. Вредоносная программа может настроить датчик на запись звуковых волн. Эти сигналы в «сыром» виде неинформативны, но после программной обработки качества записи достаточно для определения цифр от одного до десяти. Так, например, можно перехватить данные банковской карты с помощью вредоносной программы.

Кража пароля акселерометром

Сотрудники Калифорнийского университета нашли способ перехвата данных, вводимых с помощью экранной клавиатуры смартфона. Датчик ускорения (акселерометр) позволяет фиксировать все смещения, покачивания и вибрации устройства. Хао Чэнь и Лянь Цай (авторы исследования) создали программу TouchLogger, которая с помощью данных с сенсора может с 70% точностью определить нажатую цифру на телефоне. Этот метод очень сложный для реализации и требует адаптации под каждую модель смартфона, но украсть данные все же можно.

Также есть другой способ использования акселерометра для кражи данных. Его можно использовать для перехвата данных с физической клавиатуры компьютера, если телефон лежит рядом. Специальная программа позволит воссоздать виртуальную модель всех клавиш. Это возможно за счет

сравнения вибраций, создаваемых нажатием на кнопки. Таким образом, например, можно украсть несложный пароль или пин-код.

Аккумулятор может следить за вами

Некоторые браузеры, в частности Firefox, Chrome и Opera, используют интерфейс HTML5 Battery Status API, который передает информацию сайтам об уровне заряда аккумулятора в смартфоне и примерное время до разряда. Это необходимо для того, чтобы открывались облегченные версии веб-страниц для экономии энергии. Исследователи из Франции и Бельгии выяснили, что с помощью этих данных можно определить местоположение пользователя вместе с информацией о состоянии батареи.

***

17.10.2016

Ученые продемонстрировали, как АНБ прослушивает зашифрованный трафик

Бывший подрядчик Агентства национальной безопасности США Эдвард Сноуден обнародовал немало информации относительно деятельности и возможностях спецслужбы, в том числе способности перехватывать VPN-соединения и взламывать зашифрованный трафик, эксплуатируя слабые места в реализациях протокола Диффи-Хеллмана (InternetUA).

Протокол Диффи-Хеллмана повсеместно применяется для реализации HTTPS, SSH и VPN-соединений и до недавнего времени считался абсолютно надежным, однако в прошлом году исследователи обнаружили уязвимость в протоколе обмена ключами. В алгоритме применяется ограниченный набор простых чисел, часто используемых повторно. Для того чтобы взломать хотя бы одно число в 1024-битном ключе понадобится в течение года пытаться расшифровать его с помощью суперкомпьютера. Такой процесс может обойтись в сотни миллионов долларов.

Тем не менее, группе ученых из Университета Пенсильвании, французского Центра по научным исследованиям (CNRS) и Университета Лотаргинии при помощи 3 тыс. процессоров всего за два месяца удалось взломать 1024-битный ключ, что позволило им пассивно дешифровать сотни миллионов HTTPS- и TLS-соединений. Как пояснили исследователи, сам по себе алгоритм не содержит бэкдор, однако его слабое место заключается в том, как различные приложения генерируют простые числа. По словам специалистов, разработанный ими метод применим только для 1024-битных ключей.

По данным проекта SSL Pulse по состоянию на сентябрь текущего года, 22% из 140 тыс. топ-сайтов, использующих соединение по HTTPS, применяют 1024-битные ключи, которые, как оказывается, могут взломать государственные хакеры или спецслужбы вроде АНБ.

***

17.10.2016

Белый дом рассказал о рассмотрении вариантов ответа на «хакерские атаки России»

Администрация США рассматривает различные варианты ответа на действия России, которую Вашингтон обвинил в хакерских атаках и намерении подорвать выборы президента. Об этом, как передает РИА Новости, заявил официальный представитель Белого дома Джош Эрнест (InternetUA).

По его словам, президент Барак Обама «рассматривает надлежащие ответные меры в отношении попыток русских подорвать нашу политическую систему, какое бы решение ни было принято, мы вряд ли объявим о нем заранее».

Эрнест уточнил, что США не только «не объявят об это заранее но, может, никогда в этом не признаются». Он добавил, что президент «продолжает осуществлять оценку того, что совершила Россия».

Представитель Белого дома уточнил, что все возможные варианты ответных действий США «остаются на столе» и не ограничены «ответом в киберпространстве», но могут также коснуться «финансовых санкций».

***

18.10.2016

Старый троян Ghost Push вновь берется за дело

Старый троянский конь Ghost Push, в свое время подвергнувший опасности заражения около миллиона устройств под управлением Android, вновь проявил себя (Украинский телекоммуникационный портал).

Правда, на этот раз создатели вредоносного ПО выбрали менее изощренный способ его распространения, поручив «грязную работу» не утилитам из Google Play, а сайтам для взрослых.

Получив доступ к корневому сертификату, вредоносное ПО проявляется себя в виде баннера, транслирующего непрерывный поток объявлений.

Желающим избавиться от навязчивой рекламы троян предлагает отключить ее за символическую плату в несколько долларов.

Крадутся ли при этом данные пластиковых карт, доподлинно неизвестно. Несмотря на то, что создатели Ghost Push поработали над «оптимизацией» своего детища, опасность заражения им страшна далеко не всем.

Троян совместим только с устройствами под управлением ОС Android Lollipop и более ранних версий. Гаджеты, функционирующие на базе Android Marshmallow или Nougat, от проникновения Ghost Push защищены.

Если вы все-таки стали жертвой Ghost Push или имеете основания переживать за сохранность собственных данных, рекомендуем провести диагностику при помощи проверенного антивируса Ghost Push Trojan Killer.

Утилита самостоятельно обнаружит наличие заражений и, предотвратив их работоспособность, поможет провести грамотную деинсталляцию.

***

17.10.2016
Базиленко Анна
Ощадбанк попереджає про новий вид SMS-шахрайства

Ощадбанк попереджає про факти відправки підроблених SMS-повідомлень з невідомих номерів нібито від імені банку. У такий спосіб зловмисники намагаються отримати конфіденційну інформацію по платіжній картці клієнта (Watcher).

«Маємо інформацію про випадки надсилання SMS-повідомлень з різних невідомих номерів нібито від імені Ощадбанку про блокування картки та необхідність зателефонувати до Контакт-центру. Прийнявши дзвінок, зловмисники намагаються дізнатись персональні дані, зокрема номер картки», – повідомили у прес-службі.

В Ощадбанку пояснюють: співробітники банку ніколи не надсилають SMS-повідомлення і не телефонують клієнту з невідомого номера з метою отримання конфіденційної інформації по платіжній картці та не просять назвати ці дані по телефону. Користувачі карток закликають не розголошувати конфіденційну інформацію – кодове слово, номер картки, термін її дії, PIN-код, CVC / CVV-код (3 цифри на зворотному боці картки) – ні знайомим, ні стороннім, ні тим більше тим особам, які представляються співробітниками банку.

Всі SMS-повідомлення від Ощадбанку надходять за єдиним зразком: відправник повідомлення – Oschadbank, а в тексті повідомлення вказаний номер Контакт-центру банку (0800210800). Номери телефонів, з яких Ощадбанк телефонує клієнтам, такі: 38(044) 363-01-33, 38(044) 364-21-21.

***

17.10.2016
Олеся Блащук
6000 онлайн-магазинов, в том числе 67 украинских, передавали данные платежных карт мошенникам

5925 онлайн-магазинов, из которых 67 – в зоне .UA, заражены вредоносным кодом, говорит исследование голландского разработчика Виллема Де Гроота. Такая программная закладка на сервере магазина перехватывает данные платежных карт в момент их ввода пользователем в текстовое поле в браузере. В этом случае покупателей не защищает шифрование по протоколу HTTPS, так как данные перехватываются еще до шифрования (AIN.UA).

Виллем Де Гроот – сооснователь и глава безопасности голландского ecommerce-сайта byte.nl. Данные его личной пластиковой карты украли злоумышленники, поэтому он и начал свое исследование в 2015 году. Для

поиска скомпрометированных магазинов он сканировал их программное обеспечение на наличие известных фрагментов вредоносного кода.

Первые скомпрометированные сайты Гроот обнаружил в конце 2015 года. С тех пор их количество выросло как минимум вдвое. Кроме того, хакеры стали использовать все более сложные схемы для маскировки. Если раньше они использовали различные модификации одного и того же онлайн-скиммера, незначительно отличающиеся друг от друга, то сегодня Гроот обнаружил уже 9 разновидностей скрипта, принадлежащих 3 разным семействам.

«Авторы также усовершенствовали механизм перехвата данных платежных карточек. Если раньше зловред просто перехватывал страницы со строкой checkout в URL, то теперь он уже распознает популярные платежные плагины Firecheckout, Onestepcheckout и Paypal», – пишет Geektimes.

По словам голландского специалиста по безопасности, некоторые из украденных данных передавались на сервера в России. Затем похищенные данные продавались в даркнете по $30 за карту.

Онлайн-магазинам

Примечательно, что разработчики из Nightly Secure связывались с рядом зарубежных магазинов, чтобы сообщить им об онлайн-скиммере. Большинство из них либо не ответили на запрос, либо не поверили в реальность угрозы.

AIN.UA повторил этот эксперимент среди попавшего в список украинского e-commerce практически с тем же успехом. Некоторые представители онлайн-магазинов уверяли, что «недавно все почистили» и что не могут поверить в возможность онлайн-скимминга. Другие вежливо интересовались подробностями и просили выслать им более подробную информацию. Лишь один ответил, что на сайте уже ведутся работы по устранению дыр в безопасности.

«Нам пришло письмо из США, где сообщалось об этом. Мы сразу же начали делать по максимуму все, что возможно, не отключая магазин. Никого не регистрируем, проводим аудит, руками чистим по админчасти. Плюс программисты проводят необходимые обновления, убирают эти дыры», — рассказал AIN.UA Виталий, владелец магазина rossignol.kiev.ua.

Покупателям

Поскольку в список инфицированных сайтов попали 67 украинских онлайн-магазинов, AIN.UA рекомендует онлайн-покупателям:

– проверять домен онлайн-магазина на наличие в списке перед оплатой картой через интернет;

– открыть для онлайн-расчетов отдельную карту, которую пополнять только перед покупкой и лишь на необходимую сумму;

– подключить в банке сервис подтверждения онлайн-платежей при помощи пароля, приходящего в SMS (либо другой аналогичный сервис).

***

19.10.2016

У Чехії затримали росіянина, підозрюваного в кібератаках проти США

У Чехії затримали росіянина, підозрюваного в кібератаках проти США. Про це повідомляють на сайті чеської поліції (LB.ua).

За інформацією відомства, чоловіка розшукував Інтерпол. Підозрюваного затримали чеські поліцейські у співпраці з ФБР США в одному з готелів у центрі Праги, він не чинив опору.

Після затримання чоловікові стало зле, йому надали першу допомогу на місці, після чого госпіталізували.

Ім'я громадянина Росії не називають. У поліції при цьому повідомляють, що він прибув на територію Чехії разом зі своєю подругою автомобілем.

У заяві наголошено, що один із міських судів прийняв рішення про утримання росіянина під вартою. Тепер буде вирішуватися питання про його екстрадицію в США.

Улітку стало відомо про злом сервера Національного комітету Демократичної партії, а також партійного комітету з виборів до Конгресу. Демократи припустили, що атака – справа рук російських хакерів, і Москва намагається таким чином вплинути на результати голосування. 7 жовтня Міністерство внутрішньої безпеки США офіційно звинуватило російську владу в причетності до злому.

Як повідомляли 18 жовтня, США можуть ввести нові санкції проти Росії за кібератаки.

***

19.10.2016

В ЛНР и ДНР формируют группу хакеров для атак на украинские правительственные ресурсы

На Донбассе боевики формируют структурные подразделения программистов-хакеров для атак на украинские правительственные и патриотические ресурсы. Об этом 19 октября сообщил координатор группы «Информационное сопротивление» Дмитрий Тимчук (Независимое Бюро Новостей).

«В ДНР и ЛНР в составе «министерств государственной безопасности» (МГБ) по приказу кураторов из ФСБ РФ началось синхронное формирование структурных подразделений программистов-хакеров для атак на украинские правительственные и патриотические ресурсы», – написал г-н Тымчук на странице в Фейсбуке.

По его словам, прибывшие из России специалисты сейчас изучают имеющиеся в ЛНР ресурсы для проведения подобной работы.

«Одна из задач, поставленных ФСБ РФ – обеспечить тесное взаимодействие данных структурных подразделений МГБ ДНР и МГБ ЛНР, которые создаются», – подытожил господин Тымчук.

***

19.10.2016

Владислав Бухарєв працює над системою кіберзахисту України

Законодавчі ініціативи з кібербезпеки «батьківщинівця» Владислава Бухарєва підтримані сумськими науковцями та напрацьовано стратегію співпраці в цьому питанні. Таке рішення прийнято під час робочої наради з керівництвом Сумського державного університету (Сумська обласна рада).

Практичний досвід науковців та експериментальна площадка на базу ВНЗ Сумщини є важливим аспектом у створенні національної системи кібербезпеки України, переконаний народний депутат України від ВО «Батьківщина» Владислав Бухарєв.

«Сьогодні ми чітко сформували спільний план дій у питанні кіберзахисту країни. Кожен учасник наради почав працювати над своїм напрямком. Як результат, ми отримаємо ґрунтовний документ, який можна буде розглядати в українському парламенті та починати будувати ІТ- безпеку в Україні», – сказав він.

За словами депутата, Сумський державний університет має усі можливості підготувати кваліфікованих спеціалістів, які маючи законодавчу базу почнуть впроваджувати заходи на території всієї країни.

«Дуже важливою темою розмови було майбутнє вищої освіти по боротьбі з кіберзлочинністю. Країна гостро потребує молодих фахівців у цій надзвичайно актуальній сфері», – зазначив Владислав Бухарєв.

Сумські науковці розпочали практичні наукові дослідження на базі науково-дослідного навчального центру «Антикор» СумДУ за напрямком «кібербезпека». За підсумками наради створена міждисциплінарна група з науково-педагогічного складу для проведення аналізу та аудиту захищеності об’єктів інформаційної інфраструктури на вразливість до кібер-атак.

***

19.10.2016

Міноборони Росії запустило закритий військовий інтернет

Міноборони Росії завершило створення військового інтернету – комунікаційної системи під офіційною назвою «Закритий сегмент передачі даних» (ЗСПД). Про це повідомляє газета «Известия» з посиланням на представника оборонного відомства, знайомого з ситуацією (LB.ua).

«У цей момент формування мережі ЗСПД завершено. Останні роботи закінчили наприкінці літа цього року, після чого мережа функціонує в повному обсязі. Тепер ми плануємо її розширювати, встановивши додаткові термінали в військових частинах і установах», – цитує видання свого співрозмовника.

Відзначають, що військова мережа не з'єднана з глобальним інтернетом і має свій електронний поштовий сервіс, за яким дозволено передавати секретну інформацію, включаючи документи з грифом «Особливої важливості».

Джерело газети пояснило, що частково військовий інтернет розгорнуть на орендованій інфраструктурі «Ростелекому», а місцями – на власній розподіленій інфраструктурі Міноборони. У кожній військовій частині стоять сервери, які шифрують інформацію, розбивають на декілька пакетів і передають далі. Доступ у серверні приміщення строго обмежений.

За даними «Известий», у військовому інтернеті є свої сайти, які можна дивитися тільки через комп'ютери, сертифіковані службою захисту державної таємниці. Підключення до цих комп'ютерів сторонніх несертифікованих пристроїв (флеш-накопичувачів, принтерів, сканерів) неможливе, при цьому кожна спроба підключити куплену в магазині флешку контролюється спеціальним програмним забезпеченням і фіксується.

***

18.10.2016

Австралийские политики обсуждают нацбезопасность в WhatsApp

Специальный советник премьер-министра Австралии по кибербезопасности Алистер Гиббон заявил, что высшие руководящие чины страны обсуждают важные государственные вопросы с помощью мессенджера WhatsApp. Об этом сообщает Mashable (InternetUA).

Эксперты в области информзащиты выразили обеспокоенность, что конфиденциальные вопросы национальной безопасности обсуждаются с помощью обычного мессенджера. WhatsApp и схожие с ним приложения отлично подходят для быстрой связи, но сохранность передаваемых данных остается под вопросом.

Как только любая личная информация попадает в сеть WhatsApp, она потенциально может оказаться в руках хакеров, подвергая риску и отправителя, и получателя.

Особую тревогу вызывает тот факт, что WhatsApp не входит в так называемый Evaluated Products List, включающий в себя одобренные инструменты коммуникации между министерствами Австралии. Однако туда попали операционные системы Apple и Blackberry, которые используют собственные сервисы для отправки сообщений.

***

20.10.2016

Хакеры похищают данные банковских карт с помощью изображений на сайтах

Как сообщают эксперты ИБ-компании Sucuri, ни одна неделя не обходится без обнаружения нового образца вредоносного ПО для похищения данных платежных карт. Один из последних обнаруженных ими вредоносов предназначен для похищения информации клиентов online-магазинов,

работающих на базе платформы Magento. Для хранения похищенных данных программа использует стеганографию (InternetUA).

Стеганография является способом передачи или хранения информации с сохранением в тайне самого факта такой передачи. В отличие от криптографии, скрывающей содержимое сообщения, стеганография скрывает сам факт его существования. Как правило, стеганографическое сообщение будет выглядеть как что-то другое, например, как изображение.

В случае с вредоносным ПО злоумышленники прячут текстовые данные в исходном коде изображения. Подобная техника редко используется хакерами, поскольку спрятать текст внутри кода, не повредив файл, чрезвычайно сложно. Исследователи безопасности могут сразу же заподозрить неладное и проверить изображение в текстовом редакторе.

Эксперты Sucuri исследовали взломанный online-магазин, работающий на базе CMS Magento. Злоумышленники скомпрометировали файл ядра Cc.php, предназначенный для обработки данных банковских карт. Хакеры добавили в него дополнительный код, записывающий информацию, вводимую пользователями в платежную форму, и сохраняющий ее в конце локального изображения.

Что интересно, злоумышленникам удивительным образом удалось втиснуть большой объем данных платежных карт в изображение, не повредив его. Немногие хакеры, использующие стеганографию, зачастую выбирают простые изображения во избежание повреждения данных. Однако в исследованном Sucuri случае злоумышленники использовали файл с большим разрешением, который очень легко повредить. Более того, изображение было связано с продуктом, продающимся во взломанном online-магазине. Для того чтобы получить похищенные данные, хакерам достаточно лишь получить доступ к изображению, загрузить его и изъять информацию из исходного кода.

***

19.10.2016

Неизвестные взломали твиттер главы МИД Бельгии

Твиттер-аккаунт министра иностранных дел Бельгии Дидье Рейндерса был взломан неизвестными, сообщается в официальном твиттере самого министерства (InternetUA).

«Персональный твиттер-аккаунт министра иностранных дел Дидье Рейндерса был взломан. Последние сообщения, опубликованные в нем, не принадлежат министру», – говорится в тексте сообщения.

Опубликованные неизвестными сообщения носили оскорбительный характер и были обращены в адрес Канады, подписание с которой всеобъемлющего экономического и торгового соглашения ЕС блокировано региональным правительством бельгийской Валлонии.

На момент написания новости проблема была устранена, а сам министр разместил в своем блоге извинения за «доставленные неудобства», а также

картинку, на которой изображен символ Канады – кленовый лист с подписью «Храните спокойствие и любите Канаду».

***

19.10.2016
В Италии арестован сообщник лидера группировки GameOver Zeus

Сотрудники правоохранительных органов Италии арестовали россиянина, предположительно связанного с руководителем киберпреступной группировки GameOver Zeus Евгением Богачевым, разработавшим одноименный банковский троян. Как сообщает издание Softpedia со ссылкой на итальянскую полицию, по мнению правоохранительных органов, россиянин является главой местной преступной сети, занимающейся отмыванием похищенных денег (InternetUA).

По данным полиции, группировка действовала из Рима и использовала два метода перевода похищенных средств на счета своих подручных в Украине. Злоумышленники вербовали новых «сотрудников», размещая в интернете фальшивые предложения о работе, а затем предлагали им принять участие в схеме по отмыванию денег. Преступники перечисляли средства на счета новых «работников», которые затем либо обналичивали деньги, либо пересылали их на счета третьей стороны. Кроме того, преступники покупали и отправляли на домашний адрес рекрутов дорогостоящую технику и ювелирные изделия. Далее эти товары переупаковывались и отправлялись на указанные адреса в Украине.

Согласно итальянским правоохранителям, ядро группировки включало три человека – граждан России, Украины и Молдовы. Группа действовала в качестве денежных «мулов» для операторов трояна GameOver Zeus. В полиции не раскрыли, как удалось выяснить связь между итальянской группировкой и Богачевым, однако уточнили, что вышли на след преступников в ходе расследования инцидентов, связанных с использованием вредоносного ПО для хищения крупных сумм денег у ряда организаций из Болоньи.

***

19.10.2016
Вымогатель CryPy шифрует каждый файл отдельным ключем

В сети появилось новое приложение-вымогатель, на сей раз написанное на языке программирования Python. Программа CryPy (сочетание слов crypt и Python) выделяется среди других присвоением уникального ключа каждому шифруемому файлу, что значительно усложняет процесс расшифровки (InternetUA).

Используется уязвимость системы управления контентом Magento, позволяющая применять скрипт PHP уязвимого сервера в Израиле, который является командным сервером CryPy. Этот сервер используется не только для атак вымогателя, но и для фишинговых атак с поддельными сообщениями с

платёжной системы PayPal. Предположительно, родным языком авторов приложения является иврит.

CryPy состоит из двух файлов под названиями «boot_common.py» и «encryptor.py». Первый отвечает за фиксирование ошибок в системе Windows, второй является самым шифратором. При инфицировании системы отключается редактор реестра, диспетчер задач, командная строка и автозапуск. Вскоре после начинается процесс шифрования файлов пользователя.

Каждый файл получает собственный ключ шифрования. Разблокировка файлов выполняется программой дешифрования, которая находится на «секретном сервере». Каждые 6 часов один из файлов пользователей удаляется, чтобы они не затягивали с выплатой выкупа. Через 96 часов ключи удаляются и вернуть файлы будет невозможно. Лаборатория Касперского утверждает, что приложение находится на раннем этапе разработки и не способно зашифровать файлы: недавно злоумышленники переехали на новый сервер и не успели прописать его адрес в коде.

***

20.10.2016
Обнаружен преемник банковского трояна Dyre

Как сообщают эксперты компании Fidelis Cybersecurity, обнаруженный ими в прошлом месяце новый банковский троян TrickBot имеет много общего с давно известным вредоносом Dyre. Большинство операций с использованием Dyre прекратились после того, как в ноябре 2015 года российские правоохранительные органы устроили обыск в московской компании «25 этаж», занимающейся производством и дистрибуцией кинопродукции. Рассылка содержащих Dyre спам-писем прекратилась не сразу, однако после полицейского рейда стала постепенно уменьшаться, пока не снизилась почти до нуля в январе текущего года (InternetUA).

По мнению экспертов Fidelis Cybersecurity, стоящая за Dyre киберпреступная группировка или отдельные ее члены возобновили свою деятельность, используя те же методы и схожее вредоносное ПО. Прежде всего исследователи обратили внимание на то, что модуль TrickLoader, загружающий троян на систему жертвы, очень похож на загрузчик Dyre.

Правда, между двумя троянами есть и различия. TrickBot является, скорее, не клоном, а обновленной версией Dyre. Большая часть оригинального трояна написана на языке C, тогда как TrickBot – на C++, из чего можно предположить, что программы созданы разными разработчиками. С целью добиться персистентности на зараженном устройстве TrickBot использует TaskScheduler и COM, а Dyre запускает команды непосредственно на системе. Для криптографических операций новый вредонос использует Microsoft Crypto API, тогда как старый применяет алгоритмы SHA-256 и AES.

***

20.10.2016

Уязвимость в плагине угрожает сайтам на базе WordPress

Вебмастеры, по-прежнему использующие больше неподдерживаемый плагин WP Marketplace для WordPress, должны как можно скорее его удалить. Исследователи из White Fir Design обнаружили в плагине уязвимость, позволяющую загружать на сайт произвольные файлы. В зависимости от навыков и применяемых эксплоитов хакер может проэксплуатировать уязвимость и получить контроль над сервером (InternetUA).

Исследователи заподозрили неладное, когда обнаружили на различных сайтах следы сканирования на наличие CSS-файла плагина. «Запрос файла плагина, установленного на сайте, свидетельствует о том, что хакеры исследуют возможности для дальнейшей эксплуатации», – сообщили эксперты.

WP Marketplace был создан разработчиком под псевдонимом Shaon и пользовался популярностью несколько лет назад. Плагин устанавливался в online-магазинах, специализирующихся на продаже цифровой продукции. Со временем для тех же целей был создан другой плагин с более обширным функционалом – WordPress Download Manager, и Shaon объявил о прекращении поддержки WP Marketplace. Плагин получил последнее обновление порядка восьми месяцев назад. По данным WordPress.org, WP Marketplace до сих пор используется на 400-500 сайтах.

WordPress Download Manager также содержит уязвимость, позволяющую загружать произвольные файлы. Проблема была обнаружена еще в июне нынешнего года, однако до сих пор остается неисправленной.

***

20.10.2016

Інтернет-магазини по всьому світу вразив вірус, здатний викрадати гроші клієнтів

Клієнти інтернет-магазинів по всьому світу страждають через нове шкідливе програмне забезпечення, розроблене хакерами для крадіжки грошових коштів (LB.ua).

Про це повідомляє компанія Sucuri, яка спеціалізується на інформаційній безпеці.

Вірус полює за покупцями інтернет-магазинів, які працюють на популярній системі управління Magento.

Код дозволяє шахраям отримувати зображення з номерами кредитних карток і реєстраційні дані клієнта, щоб надалі дістатися до його рахунків. За даними Sucuri, вірусом заражені сайти американських, японських, турецьких і арабських онлайн-магазинів.

Щоб уникнути викрадення даних, фахівці радять використовувати якісну антивірусну програму, завести спеціальну віртуальну картку для покупок в інтернеті та вибирати надійних онлайн-ритейлерів.

***

21.10.2016

Хакерські війни: «медведєви» атакують посольства та урядові відомства

Група хакерів Fancy Bear (відома також як Sednit або «медведєви»), яку раніше пов'язували з ГРУ російського Міноборони, намагалася зламати хакерське угруповання «Шалтай-Болтай» («Анонімний інтернаціонал»), що прославилася зламами акаунтів російських чиновників (Західна інформаційна корпорація).

Про це йдеться в доповіді міжнародної компанії ESET, – пише «ТСН».

Атаки Fancy Bear були також спрямовані на українських політиків, членів опозиційної партії ПАРНАС, представників ЛДПР і російських політичних дисидентів.

«Ведмедики» намагалися зламати представників установ системи НАТО, журналістів Східної Європи, чеченські організації і академіків, які приїжджають в російські навчальні заклади. Атакам хакерів також піддавалися міністерства оборони Туреччини, України, Південної Кореї, Аргентини та республіки Бангладеш, а також посольства Алжиру, Бразилії, Колумбії, Джібуті, Індії, Іраку, КНДР, Киргизії, Лівану, М'янми, ПАР, Туркменії, ОАЕ, Узбекистану та Замбії. Цікаво, що Fancy Bear (інші її назви – APT28, Sednit, Sofacy, Pawn Storm, STRONTIUM і Tsar Team) з'явилася не пізніше 2004 року. Але за останні два роки її діяльність значно зросла і, в основному, була спрямована на атаки урядових відомств і посольств по всьому світу. Хакери з Fancy Bear «мають особливий інтерес до Східної Європі

Нагадаємо. що в червні стало відомо про злам бази даних Національного комітету Демократичної партії США. Американські власті заявили, що злом зробили російські хакери, ймовірно пов'язані з урядом РФ. У Кремлі зв'язок російської влади з хакерами неодноразово відкидали.

За даними компанії CrowdStrike, хакери з Fancy Bear мають відношення до ГРУ Міноборони Росії.

***

24.10.2016

Бельгийские СМИ атаковали хакеры после обвинений Россией в бомбардировке Алеппо

Ответственность за DDoS-атаки взяла на себя организация под названием Syrian Cyber Army. Het Nieuwsblad утверждает, что ее финансирует Россия (Экономические известия).

Хакеры атаковали бельгийские СМИ после того, как Россия обвинила Бельгию в бомбардировке Алеппо. Как говорится на сайте газеты Het Nieuwsblad, атаке подверглась она, а также газета De Standaard (сообщение об этом есть на сайте издания), информирует news.eizvestia.com.

Сайты изданий некоторое время не открывались. Сайт вещательной организации Radio Télévision Belge Francophone не работает до сих пор.

Ответственность за DDoS-атаки взяла на себя организация под названием Syrian Cyber Army. Het Nieuwsblad утверждает, что ее финансирует Россия.

Россия обвинила ВВС Бельгии в бомбардировке Алеппо 19 октября. Как заявили в российском центре по примирению враждующих сторон, днем ранее два самолета F-16 нанесли удар, в результате которого погибли шесть человек. Бельгия заявила, что ее авиация в этот день не наносила ударов. Бельгия обвинила российскую сторону в фабрикации доказательств.

***

24.10.2016

Эксперты зафиксировали новую волну атак ShellShock

В начале октября нынешнего года специалисты подразделения IBM X-Force зафиксировали новый виток атак, предполагающих эксплуатацию уязвимости ShellShock. По всей видимости, киберпреступники осуществляли атаки в разведывательных целях, пытаясь выявить устройства, уязвимые к данной проблеме. По данным специалистов, атаки осуществлялись с четырех IP-адресов (208.100.26.233, 208.100.26.235, 208.100.26.236 и 208.100.26.237) и затрагивали цели по всему миру (InternetUA).

Наибольшее число атак пришлось на Японию (35,32 %) и США (29,58 %). Далее следуют Франция (11,04 %), Великобритания (9,28 %) и Германия (6,49 %).

Напомним, об уязвимости ShellShock стало известно в сентябре 2014 года. Проблема содержится в одном из фундаментальных компонентов Linux-систем - командной оболочке bash. Уязвимость затронула не только интернет-серверы и рабочие станции, но и используемые в повседневной жизни устройства – смартфоны и планшеты, домашние маршрутизаторы, ноутбуки. В скором времени после обнаружения проблемы было выпущено исправление, однако многие владельцы серверов не спешили его устанавливать.

Как свидетельствуют данные телеметрии IBM X-Force, даже спустя два года после обнаружения ShellShock киберпреступники продолжают выказывать интерес к уязвимости – в сентябре нынешнего года было зафиксировано 20 тыс. сканирований систем на наличие ShellShock.

***

24.10.2016

В сети появился поддельный антивирус Microsoft Security Essentials

Один из последних методов сетевых мошенников основан на использовании бесплатного антивируса Microsoft Security Essentials, который доступен на системах от Windows 7 и более ранних. Компания опубликовала предупреждение, описывающее поддельный Microsoft Security Essentials,

который распознаётся антивирусами как SupportScam:MSIL/Hicurdismos.A. Цель этого вредоносного приложения – убедить пользователей в неисправности компьютера и заставить заплатить «техподдержке» за его «ремонт» (InternetUA).

Подозрение должно вызвать уже то, что под прицелом оказались пользователи систем Windows 8 и Windows 10. В реальности на этих системах используется предустановленный Windows Defender.

После установки приложение выдаёт экран BSoD, имитируя проблемы с компьютером. На экране отображается номер телефона, тогда как в настоящих сообщениях об ошибках от Microsoft никогда не содержится подобной контактной информации. BSOD создаётся при помощи сокрытия курсора мыши и отключения диспетчера задач, простым выводом изображения на весь экран. Позвонившим предлагается платное восстановление компьютера, а под видом нужных для этого программ могут быть скачаны другие вредоносные приложения.

Есть ещё несколько способов понять, что антивирус поддельный. Установочный файл называется setup.exe, но Microsoft не использует такое название для Security Essentials. В свойствах файла издателем указана не Microsoft; SmartScreen показывает уведомление, что издатель setup.exe не может быть распознан.

***

25.10.2016

Мошенники нашли новый способ обманывать банкоматы

В Украине мошенники крадут деньги из банкоматов при помощи виру сов (InternetUA).

Для взлома банкоматов мошенники используют универсальный ключ. Он подходит ко всем банкоматам одного модельного ряда. Одетые в форму работников банка, мошенники на виду у всех открывают «компьютерную» часть банкомата и внедряют вирус. Затем дожидаются приезда инкассаторов, которые заполняют банкомат деньгами.

После того, как банкомат заполнен, мошеннику достаточно подойти к банкомату под видом обычного клиента, ввести специальный код и получить наличность. Сразу и всю.

По словам начальника департамента по борьбе с киберпреступностью, полковника полиции Сергея Демедюка, банки сами виноваты в происходящем. Именно банк несет ответственность за смену универсальных замков на банкоматах. С целью экономии чаще всего банки меняют только те замки, которые контролируют «денежную» часть банкомата, его нижний отсек. При этом «мозг» устройства остается незащищенным. Ведь сигнализация также устанавливается на ту часть, где размещаются деньги.

Для работы по этой схеме мошенники создают специальные группы. Чаще всего в такую группу входят также сотрудники банка, которые владеют

информацией о местонахождении уязвимых банкоматов, графике работы инкассаторов, организации видеонаблюдения.

Правоохранители уже задержали одну такую группу. По второй ведется следствие.

«Находчивое» воровство

В эпоху таксофонов дети привязывали монетки на нитку и пользовались «неограниченным кредитом». С распространением системы мобильных терминалов эта практика вернулась в модифицированном варианте. Мошенники прикрепляют к крупной банкноте нитку, оплачивают пополнение счета, а после вытягивают деньги назад. Так, имея на руках 500-гривневую купюру, за несколько минут можно разжиться впечатляющей «прибавкой к зарплате». И уголовным преследованием вдогонку.

Шансы раскрыть киберпреступление

По словам Демедюка, киберворов находят в половине случаев. Раскрытие преступлений во многом зависит от своевременного обращения пострадавшего. Сегодня за «электронными» преступниками следит около 300 киберполицейских. При этом по штату их должно быть более 400. Так, на каждого сотрудника киберполиции в год приходится более 43 заявлений.

Ущерб от киберпреступлений в этом году за 8 месяцев составил около 27 млн грн. Более половины возмещено пострадавшим. Преимущественно киберпреступниками оказываются осужденные граждане, отбывающие тюремный срок в местах лишения свободы, и использующие для преступной деятельности телефоны с разными SIM-картами. По состоянию на конец августа было раскрыто около 1,5 тыс. преступлений.

IT-директор «ПриватБанка» Дмитрий Дубилет отметил, что «ПриватБанк» пока не сталкивался с проблемой кибервзлома банкоматов с целью снятия всего кэша за раз.

«Наиболее опасным для банков видом мошенничества остается социальный инжиниринг. Когда клиент сам передает все свои пароли и пин-коды мошеннику, который представляется милицией или СБ банка. Но здесь мы тоже понимаем, как с этим бороться», – отметил он. По словам Дубилета, службы безопасности банков пристально следят за всеми ноу-хау мошенников и стараются «играть на опережение».

***

24.10.2016

Хакерська атака вивела з ладу найбільші інтернет-сервіси

21 жовтня такі глобальні служби, як Twitter, Spotify, Airbnb і Netflix, перестали працювати (Espreso.tv).

Про це пише Tech Today.

Причиною, кажуть експерти, була потужна хакерська атака. Поки не зрозуміло, хто стояв за нападом, але вже відомо, що солдатами в ньому були чайники, принтери та інші девайси інтернету речей.

Атака була спрямована на компанію Dyn, яка надає мережеві послуги і спрямовує трафік на інтернет-сервіси. Компанія повідомила про дві DDoS-атаки на неї. Перша привела до перебоїв у роботі сервісів на дві години, і цей напад вдалося відбити. Але потім пішла друга атака і нові перебої.

Окрему атаку пережив і найбільший інтернет-магазин Amazon. У Dyn вважають, що атаки на Amazon і компанію пов'язані.

Від першої атаки постраждали в основному користувачі в Техасі й на східному узбережжі США, під час повторної – також жителі Каліфорнії і Середнього Заходу. Перебої в роботі Twitter і інтернет-кінотеатру Netflix спостерігалися і в Європі. За повідомленням порталу Gizmodo, деякі користувачі не могли потрапити на сайти найбільших світових ЗМІ, зокрема, CNN і газету Guardian. За даними порталу, перебої виникали в роботі сервісу PayPal.

Організатори нападу поки невідомі – міністерство національної безпеки США оголосило про початок розслідування. Але відомо, що постраждали соціальна мережа Twitter, музичний сервіс Spotify, сервіс бронювання нерухомості Airbnb, новинні сайти The Verge і Reddit.

Міністерство національної безпеки США також попередило, що хакери стали використовувати нові методи. Вони заражають вірусами різну техніку, серед якої модеми, принтери і пристрої на основі інтернету речей. Вони стають частиною армії ботів і беруть участь в атаці.

20 вересня 2016 року сайт відомого британського експерта з кібербезпеки Брайана Креббса KrebbsOnSecurity.com піддався найпотужнішій в історії інтернету DDoS-атаці. Це сталося після того, як Креббс викрив ізраїльську хакерську групу, яка торгувала послугами зі створення подібних атак через сервіс vDos. Він розповів про те, що оператори сервісу vDos, котрі надають послуги DDoS на замовлення, за два роки заробили понад $600 000, провівши більше 150 000 атак. Крім того, Креббс зумів встановити особи хакерів, перерахував у статті IP-адреси серверів зловмисників. Завдяки цьому хакерів заарештували, але потім випустили під заставу. Після цього на сайт Креббса обрушилася лавина трафіку.

Фахівець з кібербезпеки Брюс Шнаєр попереджає, що у близькому майбутньому можливе порушення роботи інтернету. Фахівець каже, що хтось протягом останніх двох років вивчає способи зруйнувати Павутину. Відбудеться повне відключення: пошта, веб-сайти, онлайнові сервіси. Він не знає, хто саме це планує, але каже, що зловмисники зараз проводять спрямовані DDoS-атаки, а також атаки, які дозволяють визначити, наскільки добре захищені жертви і яка повинна бути сила удару, щоб паралізувати діяльність.

***

24.10.2016

Українські хакери заявили, що зламали пошту Суркова

Група українських хакерів, що іменує себе «КіберХунта», заявила, що повністю контролює листування помічника президента РФ Владислава Суркова (InternetUA).

Про це повідомляється на сайті організації.

«Ми, українські патріоти «КіберХунта», сьогодні отримали доступ і повністю контролюємо листування одного з поштовиків ворога України В. Суркова», – йдеться у повідомленні.

Група стверджує, що зараз аналізує фрагменти листування Суркова з його помічником Карповим, який для конспірації підписує документи псевдонімом «Павлов Микола Миколайович».

Організація виклала на сайті «документи», в яких, зокрема, прописані «невідкладні комплексні заходи» з дестабілізації політичного життя в Україні.

«Досягнення викладених цілей передбачає забезпечення в найкоротші терміни заходів щодо дестабілізації політичного життя на Україні, наслідком чого мають стати дострокові парламентські і президентські вибори. Найбільш сприятливий період для реалізації розробленого комплексу заходів листопад 2016 – березень 2017», – йдеться у витягнутому хакерами «документі».

***

24.10.2016

Новое вымогательское ПО маскируется под игру Click Me

Современный рынок вымогательского ПО может похвастаться большим разнообразием. Вирусописатели словно соревнуются друг с другом в изобретательности, всячески «приукрашивая» свои творения. На днях исследователь безопасности Карстен Хан (Karsten Hahn) обнаружил очередной образец вымогательского ПО, маскирующийся под бесплатную игру Click Me (InternetUA).

После установки на систему жертвы вредонос отображает на экране кнопку с надписью «Click Me» («Кликни на меня»). Когда пользователь пытается навести на нее курсор, кнопка выскальзывает и перемещается в другое место. Пока игрок тщетно пытается поймать неуловимую кнопку, вымогатель в фоновом режиме шифрует хранящиеся на его компьютере файлы.

В настоящее время шифровальщик все еще находится на стадии разработки и лишен некоторого функционала. К примеру, пока что он может шифровать только контент в директории D:\ransom-flag.png. Вредонос использует алгоритм шифрования AES и добавляет к имени файла расширение .hacked.

Когда в попытках кликнуть на кнопку жертва нажмет на экран определенное количество раз или нажмет на Enter, появится уведомление с требованием выкупа. Сообщение содержит изображения активиста Anonymous в маске и надпись «You have been Hacked» («Вас взломали»). В уведомлении также присутствует текст на фарси с требованием оплатить выкуп за восстановление зашифрованных файлов. Еще одним свидетельством того, что

вредонос находится в стадии разработки, является отсутствие каких-либо инструкций по оплате.

***

24.10.2016

Майя Яровая

Приватности больше нет. Это война, которую мы почти проиграли – мнение эксперта

Вы все еще старательно выдумываете сложные пароли, применяете двухфакторную аутентификацию и боитесь сболтнуть лишнего в Facebook, чтобы вас не взломали? Выдыхайте, это уже произошло и довольно давно. Правда в том, что что бы вы не делали, вам не удастся защитить свои персональные данные. Но кое-что еще можно спасти. На конференции Kaspersky Security Weekend старший специалист и аналитик компании по кибербезопасности Штефан Тенеси рассказал о том, что делать, чтобы окончательно не проиграть битву человечества за приватность. AIN.UA приводит репортаж с его выступления (AIN.UA).

Я начинал свою карьеру в кибербезопасности почти десять лет назад, и мне было интересно наблюдать за тем, как меняется эта ниша. Тогда все сводилось к борьбе против кибермошенников, которые хотели завладеть нашей информацией. Сегодня на нее пытаются наложить лапу не только преступники, но также правительства, корпорации. Очень много глаз и ушей прикованы к персональным данным интернет-пользователей. Поэтому сегодня я бы хотел поговорить о приватности. Я думаю, что ее больше нет. Это битва, которую мы почти проиграли.

У всех нас (или почти у всех) есть Facebook и Twitter. Большинство из вас, скорее всего опубликовали чекин из отеля, в котором проходит эта конференция. Я не буду читать вам нотации относительно распространения вашего местоположения в социальных сетях, потому что осознаю, что это обыкновенная человеческая потребность, которой мало кто может сопротивляться. Каждый хочет быть звездой, и социальные сети отлично справляются с удовлетворением этой потребности. В Facebook каждый «сам себе селебрити» для своих фоловеров и друзей.

Но есть еще одна очень древняя и очень сильная потребность человека – это приватность. Посмотрите хотя бы на старинные изображения Адама и Евы: самое сокровенное у них прикрыто фиговыми листочками.

В книге Джорджа Оруэлла «1984» автор рисует нам картину будущего мира, в котором у каждого человека дома установлена камера и микрофон, и единственное место, где можно спрятаться от наблюдения – это угол, в котором установлена камера. Но даже когда вы там, наблюдатель знает, где вы находитесь.

Мир, в котором мы живем сегодня, не очень-то отличается от антиутопии, обрисованной Оруэллом.

В наших гостиных стоят smart-телевизоры с веб-камерой и микрофоном, подключенные к интернету. Потому что это же так удобно – общаться с кем-то в видеочате на большом экране.

Но ведь нас никто не заставлял устанавливать в своих домах эти телевизоры. Мы сделали это добровольно, своими руками. Мы купили эти телевизоры и поставили в своих гостиных. Потому что нам нравится пользоваться возможностями, которые они предлагают.

Мы больше не контролируем свои данные

Раньше, когда письма были бумажными, а покупки совершались в физических магазинах за наличные, вы могли контролировать свою приватную информацию. Но сегодня все происходит онлайн, и даже у себя дома с появлением интернета вещей вы теряете этот контроль. Ваши данные мгновенно улетают в сеть и вы больше не отвечаете за то, куда они попадают потом и как используются.

Мало кто осознает, что когда он или она открывает веб-страницу, то коммуницирует не только напрямую с веб-сервером. Когда вы открываете веб-страницу, ваш браузер отправляет десятки, сотни и тысячи запросов на самые разные серверы — для снятия статистики, для показа рекламы и т.д. То есть каждый из нас сегодня находится под наблюдением со стороны различных организаций, которые хотят получать данные о пользователях, выделять какие-то тренды, а потом монетизировать их.

Но вот что меня пугает. Вы читали новости о том, что «умной» хотят сделать даже одежду? Она будет подключена к интернету и сможет делиться тем, где мы и что делаем.

Сейчас отслеживается все, что мы делаем в интернете, но в будущем будет отслеживаться и то, что мы делаем в физическом пространстве.

Уже сегодня я вижу несколько трендов, которые заставляют меня нервничать. Например, ценовая дискриминация. Некоторые компании уже практикуют это в нескольких странах мира, в том числе в моей родной Румынии. Эти компании предлагают клиентам разные цены на один и тот же продукт, отталкиваясь от того, что они знают про этого клиента. Например, если вы покупаете билеты на самолет с компьютера Mac, вам покажут более высокую цену, чем пользователю, который делает запрос с ПК. Потому что если вы можете позволить себе Mac, значит и на путешествие можете потратить больше.

Представьте себе, как этот тренд может отразиться на таких сферах, как, например, медицинское страхование. Как думаете, что было бы, если бы ваша страховая компания заранее знала, что вы искали в интернете какое-то редкое заболевание и как его лечить? Меня нервирует, что этот тренд может стать новой общепринятой моделью ценообразования в будущем.

Кто за нами следит

Сегодня разные организации отслеживают наше поведение в интернете, чтобы таргетировать на нас рекламу. Они также отслеживают наши IP-адреса, чтобы знать, где мы находимся, ваши привычки – не сомневайтесь, если они

могут получить от вас какую-либо информацию, они попытаются это сделать. При этом все, что они делают, на 100 % легально.

Мы знаем, что у бизнесов есть доступ к нашим данным. Но он есть у кое-кого еще. Например, у этого парня:

Он выглядит как Иисус с той лишь разницей, что не приносит Спасения. Это экс-гуглер, более известный как GCreep. Довольно грустная история о 27-летнем сотруднике, который, используя служебное положение, шпионил за несовершеннолетними. У него был доступ к внутренним системам Google – всем чатам, письмам и любой интернет-активности его жертв.

Важно понимать, что когда вы даете какой-то компании доступ к вашим данным, вы также даете этот доступ всем ее сотрудникам. Но вы не можете знать, кто эти люди и насколько их помыслы чисты. И к сожалению, вы мало что можете с этим поделать. Но есть еще более опасные личности, которые также имеют доступ к нашим данным – это киберпреступники.

В 1994 году за час в киберпространстве появлялся только один новый вирус. В 2006 году новый вирус появлялся каждую минуту. В 2011-м – в секунду. Сегодня в 2016 году Kaspersky Security Lab обнаруживает 310 000 новых уникальных вирусов каждый день. Отрасль быстро растет, и если раньше атаки в основном были направлены на ПК, то сегодня под прицелом и мобильные устройства.

Все «умные» устройства, которые входят в нашу жизнь – умные телефоны, умные дома, умные автомобили, умные вещи – это части нашего будущего, в котором все аспекты жизни человека подключены к интернету и просто напросто отслеживаются. Микс из умных операционных систем, бесплатных приложений, которые мы устанавливаем на эти операционные системы, и перманентное интернет-подключение – золотая жила для киберпреступников.

Не полагайтесь на облака

Как только вы загружаете их в интернет, они уходят куда-то в облако. Облака, конечно, безопасны. По крайней мере людям нравится так думать. Но реальность такова, что облака создают люди, и люди же ими управляют. А люди склонные делать ошибки.

Эти люди могут быть сколько угодно умными и квалифицированными, но они тоже рано или поздно устают. И однажды уставший сисадмин сделает ошибку, которая приведет к масштабной утечке данных. Вопрос нужно формулировать не «если это произойдет», а «когда это произойдет». Потому что рано или поздно утечка случится.

Есть много примеров масштабных утечек из прошлого, когда фигурантом скандалов становились крупнейшие IT-компании, казалось бы, защищенные до зубов. Тогда в интернет утекли миллионы паролей от учетных записей пользователей в Last.fm, Dropbox, LinkedIn, Yahoo…

С Yahoo, кстати, это один из масштабнейших инцидентов в истории. Два года назад учетные данные практически каждого первого пользователя были скомпрометированы. Причем, известно об этом стало недавно. То есть два года

ваши персональные данные (если у вас есть аккаунт на Yahoo) свободно дрейфовали по интернету на радость хакерам.

Меня взломали?

Есть очень хороший пример того, что ваши данные и ваша личная информация больше вам не принадлежат. Это сайт Haveibeenpwned, на котором можно проверить свой аккаунт на предмет утечек. Его создал интернет-активист, который собрал воедино 155 баз данных когда-либо скомпрометированных аккаунтов. Сегодня в этой единой базе содержится почти два миллиарда взломанных аккаунтов.

Чтобы проверить, есть ли в этой базе что-то про вас, достаточно ввести в поиск email или имя пользователя. Это я и сделал. И в базе нашлось сразу пять моих аккаунтов с разных сайтов, которые были скомпрометированы: Dropbox, Last.fm, LinkedIn, а еще аккаунт на аналитической платформе Stratfor. Мне нравится изучать аналитику с геополитическими инсайтами, и я исправно платил за этот сервис, пока в 2011 году в результате его взлома в интернет не утекли мои платежные данные. Так что взломали заодно и мою кредитную карту.

Даже эксперт по кибербезопасности с огромным опытом вроде меня не застрахован от уязвимостей. Меня взломали пять раз. И это не моя вина — я все делал идеально.

Я сделал все, что мог. У меня сложные двухэтажные пароли, разные для всех сервисов. Я не кликаю ни на какие фишинговые ссылки и все равно я стал жертвой утечки данных.

Как только вы впервые заходите в интернет, вы должны понимать, что рано или поздно вас взломают, а ваши данные, ваша личная информация станет общедоступна. И вы ничего не можете с этим сделать. Разве только подать в суд на компании, которые допустили утечку. Но кто знает, что там написано в их соглашениях и политике использования, которые мы принимаем не читая? Может, они заранее предусмотрели такую возможность и сняли с себя ответственность.

Но помимо компаний, их сотрудников и хакеров доступ к вашим данным также есть у правительства. Они используют их преимущественно для того, чтобы защищать свою страну от внутренних и внешних опасностей. Правительства обеспокоены распространением шифрования, которое защищает данные пользователей от перехвата. Потому что его могут использовать не только хорошие парни, но и плохие.

В идеале если вы не хотите, чтобы какая-то секретная информация попала в интернет, просто не храните ее в онлайне.

Шифрование – наше все

Все это обыкновенное нарушение нашей приватности, и поделать ничего мы не можем. Но можем предвидеть. Я очень рад, что такая штука, как шифрование end-to-end, становится все более популярна по всему миру. Все больше интернет-сервисов устанавливают этот режим шифрования данных пользователей по умолчанию.

Проблема шифрования в том, что еще до недавнего времени это была прерогатива гиков. Большинство шифровального ПО невозможно было использовать, если только вы не один из этих полусумасшедших доморощенных хакеров, которые сидят дома и сутками копаются в компьютерах. Все изменилось после инцидента с Эдвардом Сноуденом и массивной утечки секретной информации. Стало понятно, что в идеале любая информация должна быть зашифрована. И тогда, даже если случится взлом, ничего страшного не произойдет, потому что ваши данные никто не сможет прочитать.

Я не хочу развить в вас паранойю, потому что если вы начнете сильно из-за этого париться, вы просто не сможете нормально работать.

Давайте представим себе самый безопасный в мире компьютер – каким он должен быть? Это компьютер, запертый в подвале, отсоединенный ото всех сетей и даже от розетки. Едва ли он может быть сильно полезным.

И все-таки битва пока не проиграна. Есть шифрование, и шифрование – ваш друг. Оно не обманет, не подставит, потому что это чистая математика. Если мы используем шифрование, и используете правильно, получить доступ к вашим данным становится математически невозможно.

Заходите в интернет через VPN или с помощью Tor, чтобы браузить интернет анонимно, не оставляя за собой никаких следов. Технология Fulldisk encryption пригодится, если вы много путешествуете и не хотите, чтобы власти разных стран копались в ваших данных. Используйте GPG/PGP для шифрования электронной переписки или Pidgin для чата на компьютерах Mac. Еще очень полезная штука – криптовалюты.

Объединить усилия в неравной борьбе

Инструментов много, вам лишь нужно их использовать и убедиться, что их также используют ваши друзья и родные. Потому что если они не будут этого делать, доступ к вашей информации можно получить через них. Но, к сожалению, я пока не наблюдаю массового распространения этих инструментов среди пользователей.

Давайте представим себе, что каждый облачный сервис, который вы используете, каждый веб-сайт, на который вы заходите, на 100 % безопасен. Давайте представим себе утопический Facebook, который на 100 % понятный и прозрачный в плане настроек безопасности, и все его пользователи сделали настроили все очень правильно. При этом каждый сотрудник Facebook – идеал человека, который ни за что не станет заглядывать в ваши персональные данные, а уж тем более использовать их в своих целях.

И вот один из ваших друзей инфицирован. Что это означает? А то, что вся ваша с ним переписка, все действия на его странице и даже на своей собственной теперь известны кому-то третьему. Взломав одного пользователя, хакер получает доступ ко всей информации, которая доступна этому пользователю.

В будущем, когда вся информация в мире будет зашифрована методом end-to-end, хакер сможет получить доступ только в одном месте, где она все

еще уязвима. И это место – ваш собственный компьютер, на экран которого она попадает в расшифрованном виде. Поэтому защитить ее можно, только защитив компьютер. И смартфон. Каждое ваше устройство.

Мы не можем изменить желание компаний, правительства и преступников получить доступ к нашим данным. Но мы можем изменить наше поведение в интернете. Это единственная надежда не проиграть битву за приватность.

***

25.10.2016

Екс-посол США в РФ назвав WikiLeaks «іноземним агентом»

Колишній посол США в Росії Майкл Макфол у своєму Twitter назвав ресурс WikiLeaks «іноземним агентом» (LB.ua).

«Чи можуть люди припинити називати WikiLeaks новинною організацією. Це іноземний агент, підтримуваний Росією, який публікує вкрадену інформацію», – написав він.

Макфол додав, що багато його знайомих «бояться критикувати WikiLeaks через страх бути зламаними їхніми постачальниками».

WikiLeaks відповів йому в Twitter, заявивши, що є «відзначеним нагородами незалежним ЗМІ, що повністю фінансується читачами і продажем книг і фільмів».

Раніше повідомляли, що США запідозрили Росію в передачі вкраденої інформації WikiLeaks. Телеканал CNN цитував представників спецслужб США, які заявляли про те, що «Москва щонайменше забезпечує інформацією або, можливо, безпосередньо відповідальна за витік».

***

26.10.2016

Хакеры могут получить контроль над iOS-устройствами с помощью зараженных изображений

Злоумышленники распространяют такие картинки с помощью сайтов, а также рассылают по электронной почте (Зеркало недели. Украина).

В операционной системе iOS обнаружена уязвимость, которая позволяет злоумышленникам получить контроль над устройством с помощью зараженного JPEG-изображения или PDF-файла, сообщает The Hacker News.

Хакеры распространяют подобные изображения с помощью сайтов и рассылают их по электронной почте. После загрузки подобного файла на смартфон или планшет злоумышленники могут заполучить все данные, которые хранятся на устройстве.

Apple уже устранила эту уязвимость в новой прошивке iOS 10.1, которая на этой неделе вышла на стадии бета-тестирования.

***

26.10.2016

Банковский троян GM Bot теперь может обходить защиту Android 6

Разработчик мобильного банковского трояна GM Bot выпустил новую версию вредоноса, способную обходить защиту ОС Android 6 Marshmallow. Релиз данной версии ОС состоялся в октябре прошлого года и на протяжении долгого времени считалось, что Android 6 не является уязвимой для угроз типа GM Bot и других вредоносных семейств, использующих тактику наложения поддельного контента поверх интерфейса работающих приложений (InternetUA).

По данным исследователей подразделения IBM X-Force, создатель GM Bot, известный как GanjaMan, в новой версии реализовал исходный код, позаимствованный у разработчика Джареда Раммлера (Jared Rummler), опубликовавшего его на GitHub в рамках проекта AndroidProcesses. Данный код позволяет читать контент из системного файла «/proc/» и определять запущенные приложения.

При помощи списка активных приложений атакующий может выявить недавно открытые программы, которые автоматически выводятся на передний план. Таким образом, GM Bot может выбирать и отображать подходящий поддельный интерфейс поверх настоящего приложения, тем самым повышая эффективность фишинговых операций.

Первая версия трояна GM Bot появилась в продаже на подпольных форумах в октябре 2014 года. Тогда ее стоимость составляла $5 тыс. Однако в начале февраля текущего года один из клиентов обнародовал исходный код вредоноса. В том же месяце разработчик выпустил вторую версию вредоносного ПО, написанную «с нуля». Спустя некоторое время после релиза из-за ссоры с покупателем GanjaMan стал персоной нон грата на площадках, где продавал свое вредоносное ПО. После этого он исчез из поля зрения, но, как оказалось, не навсегда.

***

27.10.2016

Мошенники активно торгуют персональными данными украинцев

Заполняя анкету в супермаркете, турфирме или даже на СТО, знайте: ваши данные спокойно могут быть переданы всем желающим. Юристы: первые суды уже есть (InternetUA).

В Украине вовсю торгуют личными данными клиентов банков, страховых компаний, турфирм, элитных ресторанов и бутиков. Буквально за 50 копеек ваши телефоны, адреса и даже коды на парадных станут доступными всем желающим. В компаниях уверяют, что на базах зарабатывают бывшие сотрудники, а в Нацполиции подтверждают: таких случаев все больше.

«Продам базу элитных ресторанов и клубов Киева, постоянные клиенты, владельцы скидочных карточек с ФИО и мобильными номерами. 8390 контактов», – гласит одно из объявлений. «База страховой компании, Киев, 2013 год, 2300 контактов», – пишет еще один продавец.

«База людей, которые размещали депозиты в валюте и гривнях, 1500 контактов», «База ВИП-персон, владельцев VISA голдкарт, владельцев авто премиум-класса». Предлагают также базы СТО, которые обслуживают «лексусы» и «тойоты», владельцев квартир и клиентов известных банков. «Вести» провели эксперимент и попытались приобрести одну такую базу от имени новой службы такси, которую мы, по легенде, хотим запускать.

«Сколько вам номеров нужно? Две-три тысячи? Без проблем, у вас там будет все указано: ФИО, точный адрес и даже код домофона в подъезде», – рассказал «Вестям» автор одного из объявлений, предложив купить три тысячи контактов жителей центра столицы всего за 210 грн.

По словам нашего собеседника, новейшей базой он обзавелся, сотрудничая с компаниями по доставке питьевой воды на дом: «Люди в курсе – они же подписывают документ об обработке персональных данных, и никто не возражает», – уверен продавец.

Банки сотрудничают со страховыми

Киевлянка Алина Маслова рассказала «Вестям», что ей периодически звонят из банка и напоминают, что срок страховки авто подходит к концу. «Звонили 1-го числа и сообщили, что 4-го истекает страховка. А буквально через 20 минут мне перезвонил сотрудник страховой и уговорил продлить страховку. Я согласилась. Они прислали мне полностью заполненные документы, включая данные об остатке на банковском счете и кредитной задолженности. Такие данные страховая не могла получить без сотрудничества с банком. Я звонила руководству банка, оставляла жалобу», – рассказала она.

Негласно сотрудники банка говорят, что начальники отделов работы с клиентами сотрудничают со страховыми, получают процент от заключенных сделок и поэтому заинтересованы в том, чтобы передавать данные клиентов. «Я уже перестал в ресторанах и бутиках оставлять свои данные. Зачем им моя фамилия, мой телефон? Хотят, чтобы я стал их клиентом – тогда только мое имя и электронный адрес для рекламы. Не хотят – до свидания», – сообщил один из бизнесменов.

Скупают оптом

Замдиректора по информбезопасности IT-компании IQusion Геннадий Гулак говорит, что чаще всего информация может уходить либо через взломы хакеров, либо же через уволенных или обиженных сотрудников.

«Уволенные лица еще некоторое время имеют доступ к данным компании. По отдельности базы, как правило, не хранят, так как иногда нужно проводить большие акции, рассылать СМС. Поэтому пока уволенный сотрудник не заблокирован, он легко может все это скачать себе», – рассказывает Гулак.

Финансовый эксперт Василий Невмержицкий также считает, что данные из банков утекают через бывших сотрудников: «Если менеджер за время работы сопровождал сто человек, то он может перейти в другой банк и использовать эти контакты. Хотя информация о клиентах попадает под понятие банковской тайны и является строго конфиденциальной».

Один из продавцов рассказал, что базы продают как сами сотрудники магазинов, ресторанов, банков, так и скупщики этих баз. «Чтобы заработать на них, я, например, имею связи с сотрудниками банков, ресторанов, СТО, супермаркетом, даже фитнес-центром. Они пополняют мои базы каждый месяц-два, за это получают небольшую плату. А я делю на элитные номера и обычные. Сейчас много колл-центров, которые продают товары по телефону. Они скупают базы оптом, за тысячу номеров 2–3 тысячи гривен», – сказал продавец.

Юристы: лишних данных лучше не оставлять

В Нацполиции говорят, что уже фиксировали случаи перепродажи личных данных, но подробностей не разглашают. Юристы же опасаются, что проданные данные могут попасть в руки мошенников или грабителей. «Там есть мобильный телефон, по которому вас можно шантажировать. А уж если есть и адрес, да еще и код на подъезде, то вашу квартиру легко ограбить, ведь они знают, что вы пользуетесь элитным СТО или ходите в дорогой ресторан», – говорит юрист Александр Карпюк.

Эксперты считают, что во многом виноваты сами клиенты.

«Получая скидочную карту или подписываясь на услуги в магазинах, вы заполняете анкету с большим количеством ненужных данных. Стоит обращать внимание на то, какие персональные данные вы оставляете и действительно ли есть в этом необходимость», – сказал «Вестям» заместитель директора по вопросам информационной безопасности Украинской межбанковской ассоциации «ЕМА» Алексей Красюк.

Строже всего обстоит дело с банковской тайной. По словам адвоката компании «Иляшев и Партнеры» Александра Выговского, банки обязаны заботиться о сохранении данных клиентов и ограничивать круг лиц, которые имеют к ним доступ.

«В случае разглашения банком банковской тайны клиент имеет право требовать от банка возмещения убытков и морального вреда. Поэтому клиент, у которого есть основания полагать, что его данные, которые он передал банку в процессе его обслуживания, попали к третьим лицам без его согласия, вправе подать в банк заявление с требованием возместить ему причиненные убытки и/или моральный вред. И даже может обратиться в суд. И такие дела, кстати, уже есть», – сообщил Выговский.

По словам адвоката, раскрытие банковской тайны может повлечь уголовную ответственность – штраф от одной до трех тысяч необлагаемых минимумов (17 000–51 000 грн). «В последнее время практика открытия уголовных дел по факту разглашения банками сведений, содержащих банковскую тайну, становится все более распространенной».

***

30.10.2016

Вымогательское ПО маскируется под лаунчер для Android

Эксперты компании Symantec рассказали о новой технике, позволяющей вымогательскому ПО Android.Lockscreen запускаться после каждой перезагрузки системы. (InternetUA).

Android.Lockscreen представляет собой вредоносную программу для Android-устройств, появившуюся в марте 2015 года. Вымогатель блокирует экран и для каждого смартфона назначает свой PIN-код . На дисплей выводится уведомление о необходимости обратиться в «техподдержку». Позвонившему по указанному номеру пользователю сообщается о необходимости оплатить услуги «техподдержки». После выплаты выкупа жертва получает PIN-код для разблокировки устройства.

По данным Symantec, новая версия Android.Lockscreen скрывает код внутри launcher.app. Лаунчеры являются частью операционной системы Android, отвечающей за управление некоторыми элементами пользовательского интерфейса. В связи с этим они автоматически запускаются при каждой перезагрузке ОС.

С выходом Android 3.1 компания Google существенно ограничила возможности для автозапуска приложений, поэтому единственный способ для вредоносного ПО получить привилегии автозапуска – это замаскироваться под лаунчер. Злоумышленники редко прибегают к такому способу, поскольку очень немногие пользователи знают, что такое лаунчеры, и еще меньше пользуются ими.

***

30.10.2016

Вредонос CloudFanta использует для загрузки файлов облачные сервисы

Исследователи компании Netskope представили подробный отчет о вредоносном ПО CloudFanta, с июля текущего года похитившем учетные данные свыше 26 тыс. пользователей. Программа распространяется с помощью фишинговых писем, содержащих вредоносное вложение или ссылку. Для хранения вредоносных файлов злоумышленники используют облачные сервисы Sugarsync и Dropbox (InternetUA).

Прикрепленный к фишинговому письму ZIP-архив NF-9944132-br.zip содержит JAR-файл NF-9944132-br.PDF.jar с двойным расширением .PDF.jar. После его открытия на систему жертвы в фоновом режиме загружаются DDL-файлы (в директорию C:\users\public). Эти файлы используют поддельное расширение .PNG и загружаются по SSL/HTTPS, что позволяет им успешно обходить межсетевые экраны и системы обнаружения вторжений. Далее файлы переименовываются и получают расширение .TWERK.

Вредонос CloudFanta предназначен для похищения учетных данных для авторизации в почтовых сервисах. Наибольшее число его жертв зафиксировано в Бразилии. Когда пользователь вводит свои логин и пароль в форму авторизации, он перенаправляется на поддельную страницу с авторизационной формой. Ничего не подозревающая жертва вводит свои данные, которые затем отсылаются на C&C-сервер, и перенаправляется обратно на настоящую страницу.

Многие банки используют для авторизации пользователей виртуальную клавиатуру, однако CloudFanta способен обходить эту меру безопасности. Вредонос делает снимки каждого нажатия и сохраняет их в текстовом файле.

Соціальні мережі

як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»

Упорядник Терещенко Ірина

Редактори: Т. Дубас, О. Федоренко, Ю. Шлапак

Свідоцтво про державну реєстрацію КВ № 5358 від 03.08.2001 р.

Видавець і виготовлювач
Національна бібліотека України
імені В. І. Вернадського
03039, м. Київ, просп. 40-річчя Жовтня, 3
Тел. (044) 524-25-48, (044) 525-61-03
E-mail: siaz2014@ukr.net
www.nbuv.gov.ua/siaz.html

Свідоцтво про внесення суб'єкта видавничої справи
до Державного реєстру видавців виготівників
і розповсюджувачів видавничої продукції
ДК № 1390 від 11.06.2003 р.